Yu.L.Ershov, E.A.Palyutin

MATHEMATICAL LOGIC

Mir Publishers

Yu. L. Ershov, E. A. Palyutin

MATHEMATICAL LOGIC

TRANSLATED FROM THE RUSSIAN
BY
VLADIMIR SHOKUROV

MIR PUBLISHERS
Moscow

Ю. Л. Ершов, Е. А. Палютин

МАТЕМАТИЧЕСКАЯ ЛОГИКА

ИЗДАТЕЛЬСТВО «НАУКА» МОСКВА

First published 1984
Revised from the 1979 Russian edition

© English translation, Mir Publishers, 1984

CONTENTS

Preface 7

INTRODUCTION 9

Chapter 1. THE PROPOSITIONAL CALCULUS 15

1. Sets and words 15
2. The language of the propositional calculus 21
3. Axiom system and rules of inference 25
4. The equivalence of formulas 32
5. Normal forms 35
6. Semantics of the propositional calculus 43
7. Characterization of provable formulas 48
8. Hilbertian propositional calculus 52
9. Conservative extension of calculi 56

Chapter 2. SET THEORY 65

10. Predicates and mappings 65
11. Partially ordered sets 70
12. Filters of Boolean algebra 78
13. The power of a set 82
14. The axiom of choice 90

Chapter 3. TRUTH ON ALGEBRAIC SYSTEMS 96

15. Algebraic systems 96
16. Formulas of the signature Σ 102
17. Compactness theorem 110

Chapter 4. THE CALCULUS OF PREDICATES 117

18. Axioms and rules of inference 117
19. The equivalence of formulas 126

20. Normal forms 130
21. Theorem on the existence of a model 132
22. Hilbertian calculus of predicates 139
23. Pure calculus of predicates 144

Chapter 5. MODEL THEORY 149

24. Elementary equivalence 149
25. Axiomatizable classes 157
26. Skolem functions 165
27. Mechanism of compatibility 168
28. Countable homogeneity and universality 181
29. Categoricity 188

Chapter 6. PROOF THEORY 198

30. The Gentzen system G 198
31. The invertibility of rules 204
32. Comparison of the calculi CP^{Σ} and G 210
33. Herbrand theorem 217
34. The calculi of resolvents 228

Chapter 7. ALGORITHMS AND RECURSIVE FUNCTIONS 236

35. Normal algorithms and Turing machines 236
36. Recursive functions 247
37. Recursively enumerable predicates 264
38. Undecidability of the calculus of predicates and Gödel's incompleteness theorem 276
List of symbols 292
Subject index 295

PREFACE

This book presents in a systematic way a number of topics in modern mathematical logic and the theory of algorithms. It can be used as both a textbook on mathematical logic for university students and a text for specialist courses.

The sections corresponding to the obligatory syllabus (Sections 1 to 9 of Chapter 1, without the small type, Sections 10 and 11 of Chapter 2, Sections 15 and 16 of Chapter 3, Sections 18 to 20, 22 and 23 of Chapter 4 and Section 35 of Chapter 7) are written more thoroughly and in more detail than the sections relating to more special questions.

The exposition of the propositional calculus and the calculus of predicates is not a conventional one, beginning as it does with a study of sequential variants of the calculi of natural deduction (although the traditional calculi, referred to as Hilbertian, also appear here). The reasons for this are:

(1) the possibility of providing a good explanation of the meaning of all the rules of inference;

(2) the possibility of acquiring more rapidly the knack of making formal proofs;

(3) a practical opportunity of making all the formal proofs necessary in the course for these calculi.

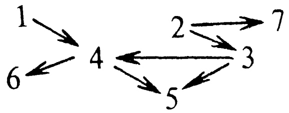
Many years' experience of the elder of the authors in reading the course of mathematical logic in the Mathematics Department of Novosibirsk State University, on which Chapters 1 to 4 are based, shows that the above possibilities are fully realizable. This justifies the use of the adopted method of presentation along with the traditional ones.

For more detail the reader is referred to the Contents.

Despite the headings Set Theory, Model Theory, Proof Theory and Algorithms and Recursive Functions, the book, being a manual, naturally contains but a small fraction of the contents of these large branches of modern mathematical logic. As is customary in textbooks, most of the results are given in the book without indicating the authors.

There is a small number of exercises after virtually each section of the book. The number of exercises, however, is obviously not enough for the purposes of teaching. The reader may find more exercises in *Problems in Set Theory, Mathematical Logic and the Theory of Algorithms* by I. A. Lavrov and L. L. Maksimova, Moscow: Nauka, 1975.

To facilitate the use of the book we indicate the interdependence of the chapters:



Some technical remarks are in order. The theorems are numbered consecutively in each chapter, the propositions and lemmas in each section. The phrase "Proposition 12.2" ("Theorem 12.2", ...) means "Proposition 2 (Theorem 2, ...) of Section 12". When referring to a proposition or lemma within the same section or, often, to a theorem within the same chapter, the section is not indicated. The symbol ⇒ stands for "implies", ⇔ stands for "is equivalent to". The symbol □ signals the end of a proof.

This book would have been impossible without the staff of the Department of Algebra and Mathematics of Novosibirsk State University. Academician A. I. Maltsev (1909-1967), an outstanding Soviet mathematician, the founder of the Department, has exercised a decisive influence upon the scientific interests and pedagogical views of the authors. At the various stages of our work at the manuscript great help and support came from M. I. Kargapolov, N. V. Belyakin, I. A. Lavrov, L. L. Maksimova and many others. We express our sincere and deep gratitude to these colleagues and friends of ours.

While preparing this book we used the notes of the courses of lectures given by A. I. Maltsev and Yu. L. Ershov, the books: *Mathematical Logic* by Yu. L. Ershov, E. A. Palyutin and M. A. Taitslin. Novosibirsk: Novosibirsk State University Press, 1973 (in Russian); *Set Theory* by K. Kuratowski and A. Mostowski. Amsterdam, 1968; *Algebraic Systems* by A. I. Maltsev. Moscow: Nauka, 1970 (in Russian); *The Theory of Algorithms* by A. A. Markov. Tr. Mat. Inst. Steklov., XLII, Moscow, 1954 (Translation: Office of Technical Services, U. S. Department of Commerce. Washington, D. C., 1962); *Mathematical Logic* by J. R. Shoenfield. Addison-Wesley, 1967, as well as other monographs and papers.

Yu. L. Ershov
Akademgorodok, Novosibirsk E. A. Palyutin

INTRODUCTION

Mathematical logic as an independent branch of modern mathematics took shape comparatively recently, at the turn of the century. The advent and rapid development of mathematical logic at the beginning of this century was associated with the so-called crisis in the foundations of mathematics. Let us consider this in some detail.

Any attempt at a systematic presentation of mathematics (or of any other science, for that matter) leads to the problem of choosing basic (primitive) notions and principles to base the entire presentation on. The problem of choosing and justifying the choice of the initial data lies as a rule outside the discipline itself and relates to the philosophy and methodology of science. The systematization of mathematics in the late nineteenth century revealed that very promising is the use of the notion of set as the only primary notion for the whole of mathematics. The work of B. Bolzano, R. Dedekind and G. Cantor led to the creation of a new mathematical discipline, the theory of sets, the beauty and force of whose constructions and the prospects of using it in the foundations of mathematics attracted the attention of many leading mathematicians of that time. Much work was done to give a set-theoretic interpretation to mathematical and even logical notions. Of great interest in this connection are the investigations of G. Frege and B. Russell. However, a high degree of abstraction and the "universality" of the concept of set could not but lead finally to the difficulties that are well and long known in philosophy when working with "universals". This manifested itself in the appearance of the so-called set-theoretic paradoxes.

Here is one of the most typical set-theoretic paradoxes, the Russell paradox: quite meaningful for an arbitrary set is the question, "Will that set be an element of itself?" An example of a set containing itself as an element could be, for instance, the set of all sets. Consider the set M_0 of all sets for which the answer to the question is "no". Now ask if the set is its own element. To our (naive) surprise we discover that if the answer is "yes", then we have $M_0 \in M_0$, i. e. the answer must (should) be "no". But if the answer is "no", then by virtue of the definition of the set M_0 the answer must be "yes". This paradox shows that unless we want to come to contradictions it is necessary (in particular) to relinquish the pleasant idea that any meaningful condition on the elements defines some set. Fortunately, paradoxes of this sort may arise only for "large" or "unnatural" sets one may well do without in mathematics *.

The appearance of such paradoxes was regarded with apprehension by many mathematicians and therefore attracted to the questions of the foundations of mathematics close attention of practically all leading mathematicians of that time (D. Hilbert, H. Poincaré, H. Weyl, to name only a few). Several programmes of "saving" mathematics from the "horrors" of paradoxes were proposed into which we shall not go here. We shall describe in brief below just two of the most effective programmes various modifications of which are still being discussed at present. We only note here that the variety of the approaches to the foundations of mathematics has remained up to the present time. However, the years past and the undeniable achievements of mathematical logic, which are yet to be discussed, made this problem lose its edge to such an extent that most of the mathematicians working in other areas of mathematics give no particular attention to the discussions now taking place among the specialists in the foundations of mathematics.

One of the most elaborate programmes of the foundations of mathematics is D. Hilbert's programme of finitary justification of mathematics. The programme is essentially an attempt to construct such a formalization of mathematics that it would be possible to prove a system's own consistency by means of the system.

---

* The formalizations of set theory to be mentioned below, axiomatic set theories, while retaining all that is useful, do not allow any of the known "paradoxical" arguments to be conducted.

Another fundamental requirement of such a formalization is that the primitive and immediately verifiable statements about the natural numbers should be true in that formalization. The work at that programme done by both Hilbert himself and by his disciples and followers turned out to be very fruitful for mathematical logic, in particular in the development of the modern axiomatic method. Although the programme of "finitism" turned out to be impracticable in its original form, as was shown by K. Gödel in his famous works, possible modifications of the programme continue to be usefully discussed up to the present time.

Another approach to the foundations of mathematics was due to the criticism of a number of positions that were used in mathematics without due justification. This relates, in particular, to the unlimited use of the law of excluded middle and the axiom of choice. The programme of constructing mathematics under rigid restrictions on the use of these principles has been given the name of intuitionism; its creation and development is due in the first place to L. E. J. Brouwer. The constructive approach to the foundations of mathematics which is being developed in the Soviet Union by A. A. Markov and his school is also due to a critical approach to admissible logical means in mathematics and uses in a systematic manner the concept of algorithm for constructive reproduction of mathematical results.

Although the foundations of mathematics are traditionally referred to mathematical logic, it is out of place in the present textbook to go into particulars of this area lying on the border of mathematics and philosophy. Therefore we restrict the discussion of the foundations of mathematics to the above remarks that do not pretend to be complete or exhaustively precise but rather serve the purposes of illustration.

The main outcome of the activities in the realm of the foundations of mathematics is, it seems, the formation of mathematical logic as an independent mathematical discipline and the fundamental achievement of mathematical logic is the development of the *modern axiomatic method* which is characterized by the following three features:

1. Explicit formulation of the postulates (axioms) of one theory or another.

2. Explicit formulation of logical means (rules of inference) admitted for a consistent construction (development) of that theory.

3. The use of artificially constructed formal languages for the presentation of all the positions (theorems) of the theory under consideration.

The first feature characterizes the classical axiomatic method. The next two are further steps in achieving maximum precision and clarity in presenting theories. Introduction and use of suitable notation was throughout the history of mathematics a very important and productive procedure. But mathematical symbols were merely elements of formal languages. In mathematical logic, on the other hand, for the first time in history such rich formal languages were created that allow practically all basic positions of modern mathematics to be formulated. The rich formal languages of mathematical logic and the successful experience of working with them have created one of the objective prerequisites for the creation of universal computing machines employing at present a very diverse spectrum of formal programming languages.

The main object of study in mathematical logic are various calculi. The notion of calculus comprises such basic components as: (a) the (formal) language of the calculus; (b) the axioms of the calculus; (c) the rules of inference. The concept of calculus allows us to give a strict mathematical definition of the nótion of *proof* and to obtain precise statements about the impossibility of proving one proposition or another of a theory. Another remarkable achievement of mathematical logic is the discovery of a mathematical definition of the notion of *algorithm*, i. e. effective procedure for solving problems of one (infinite) class or another. Intuitively the concept of algorithm has been used for a very long time. G. W. Leibniz, an outstanding thinker (1646-1716), even dreamt of discovering a universal algorithm for solving all mathematical problems. The precise definition of the notion of algorithm shattered rather quickly this beautiful Utopia; A. Church showed in 1936 that no algorithm is possible which given an arbitrary statement written in a formal language of elementary arithmetic would answer the question, "Will the statement be true for the natural numbers?" It was later found that even in the system describing "pure logic" (the calculus of predicates) the problem of provability was algorithmically unsolvable. In the subsequent years a great many algorithmically unsolvable problems were discovered in many branches of mathematics. A great contribution to the development of the theory of algorithms and to the solution of algorithmic problems has been made by E. L. Post, A. M. Turing, S. C. Kleene and the Soviet mathematicians A. I. Maltsev, P. S. Novikov and A. A. Markov.

The study of calculi constitutes the *syntactical* part of mathematical logic. The deepest study of the (syntactical) notion of proof in calculi makes an independent branch of mathematical logic known as *proof theory*. Along with the syntactical study of calculi, there is also a *semantic* study of the formal languages of mathematical logic. The basic concept of semantics is the notion of truth for the expressions (formulas, sequents and so on) of a formal language. Semantic notions have also received precise mathematical definitions, which has made possible a systematic and rigorous study of the various concepts of truth. The classical semantics of the language of the calculus of predicates has constituted a very rich branch of mathematical logic, *model theory*, which is being actively developed, and its methods and results are used to advantage in other branches of mathematics (algebra, analysis). The founders of model theory are A. Tarski and A. I. Maltsev.

Calculi allow many parts of mathematics and of other sciences to be formalized. The propositional calculus and the calculus of predicates mentioned above are formalizations of logic, the oldest science about the laws of correct reasoning. The creation and study of these formalizations have been an important stage in the development of logic as a science. The early attempts to formalize logic are due to Aristotle and G. Boole, but it was not until the advent of mathematical logic that an actual (and effective) formalization of logic was brought about. The Italian mathematician G. Peano has done much for the development and popularization of formal languages of logic.

It was the possibility of formalizing the theory of sets that proved especially important for mathematics. The calculi formalizing the basic constructions of "naive" set theory turned out to be so rich that any set-theoretic argument occurring in actual mathematical practice could be reconstructed formally in those calculi. The natural "payment" for this richness was Gödel's discovery of the effects of incompleteness and even of non-completability of such calculi.

In constructing the semantics of natural or formal languages there are also great difficulties. Thus the simple-minded belief that every declarative sentence in English can be assigned in a plausible (or at least consistent) way a truth value is refuted by the so-called Liar paradox. A man says, "What I am saying is false". Let us try to find out whether the man told the truth or a lie. If we suppose that he told the truth, then it follows from the meaning of his words that he told a lie. If he told a lie, then from the fact that his words are false it follows that he told the truth. This paradox underlies a number of remarkable theorems of mathematical logic (theorems of incompleteness and indeterminability of truth in a system).

The history of mathematical logic is a subject in its own right and it will be given no attention in this book, except for the above, clearly incomplete, listing of some names and facts.

In conclusion it should be noted that modern mathematical logic is a large and ramified branch of mathematics whose source of problems, along with its intrinsic problems, is constituted by both philosophical problems of the foundations of mathematics and logic and problems arising in other branches of mathematics (algebra, analysis, mathematical cybernetics, programming and so on).

Chapter 1

THE PROPOSITIONAL CALCULUS

1. SETS AND WORDS

By a *letter* we mean a sign regarded as a whole, i. e. a sign whose parts we are not interested in. A letter will also be called a *symbol* *. Two given (for example, written) letters can be said to be the same or distinct. For example, all small letters "a" in this book are considered to be the same. So are all small letters "a" in some hand-written text, although the sameness of two letters is more difficult to establish in this case than in the previous one. It will be assumed that it is always possible to establish the sameness of or distinction between two concrete letters under consideration. If letters a_1 and a_2 are the same, then we shall write $a_1 = a_2$.

The abstraction of identifying the same letters leads to the notion of *abstract letter*. In what follows the same two concrete letters a_1 and a_2 will be treated as the same (abstract) letter a. Each of these two concrete letters will be called a *representative* of the abstract letter a **.

A collection X of some objects, to be called elements of X, will be called a *set* ***.

If a is an element of X, then we write $a \in X$. If any element of X is an element of a set Y, then X is said to be a *subset* of Y and this is designated as: $X \subseteq Y$. If for the sets X and Y we have $X \subseteq Y$ and $Y \subseteq X$, then we shall say that the sets X and Y are equal and write $X = Y$. Thus a set is completely determined by its elements. In particular, there is only one set containing no elements. Such a set will be called *empty* and designated $\varnothing$. If $a \in X$ fails for X, then we shall write $a \notin X$.

---

* Sometimes the word "letter" will be used in its usual sense, for example Latin letter, small letter.

** One should distinguish between the abstract letter denoted by the symbol a and the symbol a itself which is a designation or name of the abstract letter.

*** As noted in the Introduction, such a definition may in general lead to a contradiction. This must not frighten the reader, however, since the existence of all the sets considered in this book can be derived within the formal system described in Section 11, in which it is impossible to carry out any of the known "paradoxical" arguments about sets.

The letters $i, j, k, l, m, n, p, r, s$, possibly with indices, will denote natural numbers. The set of all natural numbers will be denoted by ω. If $a_1 \in X, \ldots, a_n \in X$, then we shall write $a_1, \ldots, a_n \in X$. If X is a set, $a_1, \ldots, a_n \in X$ and any element of X is equal to one of the $a_1, \ldots, a_n$, then we shall say that X is a *finite set* and write $X = \{a_1, \ldots, a_n\}$ *. If $\varphi(a)$ is some condition on the object a and X is a set, then by $\{a \in X \mid \varphi(a)\}$ or $\{a \mid \varphi(a), a \in X\}$ we denote the set containing as its elements those and only those elements $a \in X$ which satisfy the condition $\varphi(a)$. For example, $\{n \in \omega \mid n = 2k \text{ for some } k \in \omega\}$ is the set of all even natural numbers.

A set of abstract letters is called an *alphabet*. A letter which is an element of an alphabet A will be called a *letter of the alphabet* A.

A finite series of concrete letters written one after the other is called a *concrete word*. In particular, each concrete letter is a concrete word. If each letter of a concrete word is a representative of some letter of the alphabet A, then we shall say that α is a *word in the alphabet* A. It is also possible that a word α contains no concrete letter. Such a word will be called *empty* and denoted by Λ. We shall say that two concrete words $a_1 \ldots a_n$ and $b_1 \ldots b_k$ of A are equal and write $a_1 \ldots a_n = b_1 \ldots b_k$ if $n = k$ and $a_1 = b_1, \ldots, a_n = b_n$. All empty words are assumed to be equal. If $a_1 \ldots a_n$ is a concrete word consisting of n letters $a_1, \ldots, a_n$ of A, then n is said to be the *length* of that word. The length of an empty word is the number 0.

Applying the abstraction of identification, two equal concrete words α_1, α_2 will be said to be the same (abstract) word α. The two concrete words will be called *representatives of the word* α. It follows from the definition of equality of two concrete words that the abstract word α may be defined to be a finite series of abstract letters such that each representative of α is a series of representatives of the corresponding abstract letters. The number of abstract letters in that series will be called the *length of the abstract word* α. An empty abstract word will be denoted by the same letter Λ as concrete empty words.

---

* Note that a pairwise distinction of the elements $a_1, \ldots, a_n$ is not assumed. In particular, $\{\varnothing\} = \{\varnothing, \varnothing, \varnothing\}$.

For abstract words α and β we define an abstract word $\alpha\beta$ to be such an abstract word all of whose representatives are obtained by writing after some representative of α some representative of β. The abstract word $\alpha\beta$ will be called the *union* of α, β; the abstract word α will be called the *beginning* of $\alpha\beta$. Similarly defined is the union $\alpha_1 \ldots \alpha_n$ of the abstract words $\alpha_1, \ldots, \alpha_n$.

In what follows, by a word we mean an abstract word. It is obvious that for any words α and β we have $\Lambda\alpha = \alpha\Lambda = \alpha$ and $\alpha\Lambda\beta = \alpha\beta$.

A word β of A is said to be a *subword* of a word α of A if $\alpha = \gamma\beta\delta$ for some words γ, δ. In particular, any beginning of α will be a subword of α. It may turn out that $\alpha = \gamma\beta\delta = \gamma_1\beta\delta_1$ and $\gamma \neq \gamma_1$. In this case we speak of distinct *occurrences* of the subword β in α. Thus an occurrence of β in α is the word β together with its position in α. An occurrence of the word β in α can be represented as: $\gamma * \beta * \delta$, where $*$ is a symbol exterior to the alphabet A. In particular, if $\alpha = \gamma\beta\delta = \gamma_1\beta\delta_1$ and $\gamma \neq \gamma_1$, then we have two distinct occurrences $\gamma * \beta * \delta$ and $\gamma_1 * \beta * \delta_1$ of β in α. If for the occurrence of $\gamma_0 * \beta * \delta_0$ of β in α the word γ_0 (the word δ_0) has the smallest length among all the words γ (the words δ) for which $\alpha = \gamma\beta\delta$, then $\gamma_0 * \beta * \delta_0$ is said to be the *first* (*last*) *occurrence* of β in α.

An *occurrence of a letter a in* α is the occurrence in α of the word consisting of a single letter a. If there is an occurrence of a letter a in the word α, then we say that the *letter a occurs in* α.

Let $\gamma * \beta * \delta$ be an occurrence of the word β in α. If $\alpha' = \gamma\beta'\delta$ for some word β', then we shall say that the word α' is obtained from α by *replacing the occurrence* $\gamma * \beta * \delta$ *of the subword by the word* β'.

A series $X_1, \ldots, X_n$ of some objects X_i, $i \in \{1, \ldots, n\}$, will be called a *sequence* or *suite*, and n is the *length* of the sequence. The objects X_i, $i \in \{1, \ldots, n\}$ will be called *terms* or *elements* of the sequence $X_1, \ldots, X_n$. It is assumed that from the notation of a sequence its terms and their order are uniquely reconstructed. To do this it is necessary for us to separate the terms, for example with a comma. If $n = 0$, then $X_1, \ldots, X_n$ will be said to be an empty sequence and designated by the same symbol $\varnothing$ as an empty set. The sequence $X_1, \ldots, X_n$ will sometimes be denoted by $\langle X_1, \ldots \ldots, X_n \rangle$. If $X_1, \ldots, X_n$ are sets, then the set of all sequences $\langle a_1, \ldots, a_n \rangle$, where $a_1 \in X_1, \ldots, a_n \in X_n$, will be denoted by $X_1 \times \ldots \times X_n$. If $X_1 = X_2 = \ldots = X_n$, then the set $X_1 \times \times X_2 \times \ldots \times X_n$ will be alternatively denoted by X_1^n. A sequence of two (three and so on) terms will be called a *pair* (*triple* and so on). A sequence of n elements will be called an *n-tuple*.

The *mapping* f of a set X into a set Y is a correspondence associating with each element $a \in X$ an element $f(a) \in Y$ called the *value* of f at a. It is clear that the mapping f of X into Y is uniquely defined by the set $\{\langle a, f(a)\rangle \in X \times Y \mid a \in X\}$. This set sometimes called the graph of f will be identified with the mapping f. If f is a mapping of X into Y, then we write $f\colon X \to Y$. If X is a set, then any mapping $f\colon X^n \to X$ will be said to be an *n-place operation* on X and n will be said to be the *number of places* in the operation f. If $f\colon Y \to X$ and $Y \subseteq X^n$, then f will be called a *partial n-place operation on X* with domain of definition Y.

Let X be a set, $X_0 \subseteq X$ and $f_1, \ldots, f_k$ be operations on X the numbers of places in which are $n_1, \ldots, n_k$ respectively. We define the set $W \subseteq X$ as follows: $a \in W$ if and only if there is a sequence $a_0, \ldots, a_m$ of elements of X having the following property: $a_m = a$ and for any $i \leqslant m$ either $a_i \in X_0$ or $a_i = f_j(a_{i1}, \ldots, a_{in_j})$ for some $j \in \{1, \ldots, k\}$ and some $i_1, \ldots, i_{n_j} < i$. In this case we shall say that the set *W is defined by induction using the following definition*:

(1) *if* $a \in X_0$, *then* $a \in W$;

(2) *if* $i \in \{1, \ldots, k\}$ *and* $a_1, \ldots, a_{n_i} \in W$, *then* $f_i(a_1, \ldots \ldots, a_{n_i}) \in W$.

We shall say that a *calculus I* is given, if the following four sets are given:

(a) an alphabet $A(I)$;

(b) a set $E(I)$ of words of $A(I)$ called a *set of expressions of I*;

(c) a set $A\mathrm{x}(I)$ of expressions of I called the set of *axioms for I*;

(d) a set $\{f_1, \ldots, f_n\}$ of partial operations on $E(I)$ called the *rules of inference of I*.

Expressions of the calculi to be considered in this book will be called *sequents* and *formulas* and the rules of inference f: $Y \to E(I)$ will be written thus:

$$\frac{\Phi_0, \ldots, \Phi_n}{f(\Phi_0, \ldots, \Phi_n)}\ .$$

The domain of f is indicated unless it coincides with $(E(I))^n$. The expressions $\Phi_0, \ldots, \Phi_n$ in the previous notation will be called *hypotheses* and the expression $f(\Phi_0, \ldots, \Phi_n)$ is the *conclusion* of a rule f. An n-place rule f of the calculus I will also be called an n-hypothesis rule. The pair $\langle A(I), E(I)\rangle$ consisting of the alphabet $A(I)$ and the set of expressions $E(I)$ of I will be called the *language* of I and denoted by $L(I)$. Suppose that two calculi I_1 and I_2 are given. If $A(I_1) \subseteq A(I_2)$ and $E(I_1) \subseteq E(I_2)$, then we shall say that the language $L(I_2)$ of the calculus I_2 is an *extension* of the language $L(I_1)$ of the calculus I and write as follows: $L(I_2) \subseteq \subseteq L(I_1)$ *.

If the calculus I is given, then the set $T(I) \subseteq E(I)$ of *provable expressions* or *theorems* of I is defined using the following inductive definition:

(1) if S is an axiom of I, then S is a theorem of I;

(2) if $S_1, \ldots, S_n$ are theorems of I, f is an n-hypothesis rule of I and $\langle S_1, \ldots, S_n\rangle$ is in the domain of f, then $f(S_1, \ldots, S_n)$ is a theorem of I.

To define a set X it suffices to indicate for what objects a the relation $a \in X$ is true. Therefore the following expressions will be uniquely defined by two sets X and Y new sets $X \cap Y$, $X \cup Y$, and $X \setminus Y$ called respectively the *intersection*, *union* and *difference* of the sets X and Y:

(a) $a \in X \cap Y \Leftrightarrow (a \in X$ and $a \in Y)$;

(b) $a \in X \cup Y \Leftrightarrow (a \in X$ or $a \in Y)$;

(c) $a \in X \setminus Y \Leftrightarrow (a \in X$ and $a \notin Y)$.

PROPOSITION 1. *The operations of intersection and union satisfy the following equations for any sets X, Y and Z:*

$$\left.\begin{array}{l} \text{1a. } X \cap Y = Y \cap X, \\ \text{1b. } X \cup Y = Y \cup X \end{array}\right\} \quad (\textit{commutativity});$$

---

* This notation does not entirely agree with the already introduced inclusion notation for sets, yet it is convenient and causes no confusion.

$$\left.\begin{array}{l}\text{2a. } X \cap X = X,\\ \text{2b. } X \cup X = X\end{array}\right\} \quad (\textit{idempotency});$$

$$\left.\begin{array}{l}\text{3a. } (X \cap Y) \cap Z = X \cap (Y \cap Z),\\ \text{3b. } (X \cup Y) \cup Z = X \cup (Y \cup Z)\end{array}\right\} \quad (\textit{associativity});$$

$$\left.\begin{array}{l}\text{4a. } X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z),\\ \text{4b. } X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)\end{array}\right\} \quad (\textit{distributivity}).$$

Checking these equations presents no difficulty. We prove 4b, for example. Let a be on the left of the equation. Then $a \in X$ or $a \in Y \cap Z$, therefore $a \in X \cup Y$ and $a \in X \cup Z$, i. e. a is at the right. If $a \in X \cup Y$ and $a \in X \cup Z$, then $a \in X$ or $a \in Y \cap Z$. Consequently, a is on the left of 4b. □

If X is a set, then the set of all of its subsets is said to be the *power set* of X and is denoted by $P(X)$.

Let J be a nonempty set and X_i, for $i \in J$, be some sets. The *union* $\bigcup_{i \in J} X_i$ and *intersection* $\bigcap_{i \in J} X_i$ of the sets X_i, $i \in J$, will be the sets defined as follows:

$$a \in \bigcup_{i \in J} X_i \Leftrightarrow (a \in X_i \text{ for some } i \in J),$$

$$a \in \bigcap_{i \in J} X_i \Leftrightarrow (a \in X_i \text{ for all } i \in J).$$

If $X_0, \ldots, X_n, Y$ are sets, then the notation $X_0, \ldots, X_n \to Y$ will mean that $\bigcap_{i \leqslant n} X_i \subseteq Y$ and $X_0, \ldots, X_n \to$ will mean that $\bigcap_{i \leqslant n} X_i = \varnothing$. If $\Phi_0, \ldots, \Phi_n, \Psi$ are some statements, then the notation

$$\frac{\Phi_0, \ldots, \Phi_n}{\Psi}$$

will mean that either one of the statements $\Phi_0, \ldots, \Phi_n$ is false or Ψ is true.

PROPOSITION 2. *Let $X_0, \ldots, X_n, Y_1, Y_2, Z$ be sets. Then*

$$(1)\ \frac{X_0, \ldots, X_n \to Y_1;\ X_0, \ldots, X_n \to Y_2}{X_0, \ldots, X_n \to Y_1 \cap Y_2};$$

$$(2)\ \frac{X_0, \ldots, X_n, Y_1 \to Z;\ X_0, \ldots, X_n, Y_2 \to Z;\ X_0, \ldots, X_n \to Y_1 \cup Y_2}{X_0, \ldots, X_n \to Z}.$$

PROOF. Let $a \in \bigcap_{i \leqslant n} X_i$. From the truth of the statements of (1) above the line we have $a \in Y_1$,and $a \in Y_2$, i. e. $a \in Y_1 \cap Y_2$. Suppose now that the statements of (2) above the line are true and $a \in \bigcap_{i \leqslant n} X_i$. From the third statement above the line it follows that $a \in Y_1 \cup Y_2$, i. e. $a \in Y_1$ or $a \in Y_2$. In both cases, from the truth of the first two statements above the line we get $a \in Z$. ☐

Exercises

1. How many distinct occurrences has an empty word Λ in a word of length n?

2. Show that the number of distinct subwords of a word α of length n is at most $\frac{n(n+1)}{2} + 1$.

3. For what words α of length n is the number of distinct subwords of α $\frac{n(n+1)}{2} + 1$?

4. Let the sets $X_0, \ldots, X_{n+1}$ be subsets of some set Y. Denote by $\overline{X}_i$ the set $Y \setminus X_i$. Show that:

(a) $\overline{\bigcup_{i \leqslant n} X_i} = \bigcap_{i \leqslant n} \overline{X}_i$;

(b) $\overline{\bigcap_{i \leqslant n} X_i} = \bigcup_{i \leqslant n} \overline{X}_i$;

(c) $\dfrac{X_0, \ldots, X_n, \overline{X}_{n+1} \rightarrow}{X_0, \ldots, X_n \rightarrow X_{n+1}}$;

(d) $\dfrac{X_0, \ldots, X_n \rightarrow X_{n+1}}{X_0, \ldots, X_n, \overline{X}_{n+1} \rightarrow}$;

(e) $X_0 \cap X_1 = X_0 \setminus (X_0 \setminus X_1)$.

2. THE LANGUAGE OF THE PROPOSITIONAL CALCULUS

A proposition in the English language is a statement, a declarative sentence which can be said to be true or false. For example, the proposition "water is a product of hydrogen combustion" is true and the proposition "all odd natural numbers are primes" is false. From propositions A, B in English we can form more complex propositions, such as "*A* and *B*", "*A* or *B*", "it is false that *A*", "if *A*, then *B*". If we know whether each of the propositions *A* and *B* is true or false, then we can determine whether the above compound propositions are true or false. For example, if *A* is true and *B* is false, then the proposition "if *A*, then *B*" is false. However, we can sometimes assert the truth of a compound proposition without knowing whether the component propositions are true or false. For example, whatever propositions *A* and *B* may be, "it is false that *A* or if *B*, then *A*" is always true. In this case we say that the scheme "it is false that *A* or if *B*, then *A*" is identically true. One of the main problems of the propositional calculus to study which we now proceed is the description of identically true schemes. To do this one will have to replace English by a formal language that allows no ambiguities.

The alphabet of the propositional calculus (abbreviated PC) consists of three groups of symbols.

1. Propositional variables: Q_0, Q_1, ..., Q_n, ..., where n is a natural number.

2. Logical symbols or connectives: $\rightarrow$, $\wedge$, $\vee$, $\neg$, $\vdash$ called respectively the implication sign, the conjunction sign, the disjunction sign, the negation sign and the turnstile or the yield sign.

3. Auxiliary symbols: left parenthesis (, right parenthesis) and a comma ,.

DEFINITION. A *formula of* PC is a word of the alphabet of PC satisfying the following inductive definition.

1. A propositional variable is a formula (we shall call it *elementary* or *atomic*).

2. If Φ and Ψ are formulas, then $(\Phi \wedge \Psi)$, $(\Phi \vee \Psi)$, $(\Phi \rightarrow \Psi)$ and $\neg \Phi$ are formulas.

It follows from the definition that $(Q_0 \wedge Q_1) \vee Q_0$ is not a formula (there are no outer brackets). To abbreviate the notation, however, we shall often drop outer brackets. Thus $(Q_0 \wedge Q_1) \vee$ $\vee\, Q_0$ will be an abbreviation of the formula $((Q_0 \wedge Q_1) \vee Q_0)$.

In what follows formulas of the propositional calculus will be denoted by the letters Φ, Ψ, X and propositional variables by P, R, with Φ, Ψ, X, P, R allowed to have indices.

A *subformula* Ψ of a formula Φ of PC is a subword of Φ which is a formula of PC.

We now prove the statement about the uniqueness of the decomposition of a formula of PC.

PROPOSITON 1. *Any nonatomic formula* Φ *of PC is representable in one and only one of the following forms*: $(\Psi \wedge X)$, $(\Psi \vee X)$, $(\Psi \rightarrow X)$ *or* $\neg \Psi$ *for uniquely defined formulas* Ψ *and* X.

To prove the proposition we first need to establish one technical fact.

LEMMA 1. *If* Φ *and* Ψ *are formulas of* PC *and* Φ *is the beginning of* Ψ, *then* $\Phi = \Psi$.

PROOF. We shall prove the lemma by induction on the length of Φ. If Φ is atomic, then so must be Ψ since otherwise Ψ begins with parenthesis or $\neg$ and then Φ cannot be the beginning of Ψ. Hence $\Phi = \Psi$.

Suppose that Φ is nonatomic and has the form $\neg\Phi'$, then Ψ must have the form $\neg\Psi'$, and, as can be easily seen from the definition of a formula, Φ' and Ψ' must be formulas. Moreover, Φ' is obviously the beginning of Ψ'. By the induction hypothesis $\Phi' = \Psi'$ and hence $\Phi = \neg\Phi' = \neg\Psi' = \Psi$.

Let Φ be of the form $(\Phi_0 \tau \Phi_1)$, where Φ_0 and Φ_1 are formulas of PC, τ is one of the signs $\wedge$, $\vee$, $\rightarrow$. Then Ψ begins with a parenthesis (and can therefore be represented as $(\Psi_0 \tau' \Psi_1)$, where Ψ_0 and Ψ_1 are formulas and τ' is one of the signs $\wedge$, $\vee$, $\rightarrow$. Since $(\Phi_0 \tau \Phi_1)$ is the beginning of $(\Psi_0 \tau' \Psi_1)$, the word Φ_0 is the beginning of the word $\Psi_0 \tau' \Psi_1$ and Ψ_0 is also the beginning of that word. Of the two beginnings of the same word one is the beginning of the other (one must take the beginning of the smaller length). Hence Φ_0 is the beginning of Ψ_0 or Ψ_0 is the beginning of Φ_0. In any case one can apply the induction hypothesis and hence $\Phi_0 = \Psi_0$, $\tau = \tau'$ and Φ_1 is the beginning of Ψ_1. Again, applying the induction hypothesis we get $\Phi_1 = \Psi_1$ and $\Phi = (\Phi_0 \tau \Phi_1) = (\Psi_0 \tau' \Psi_1) = \Psi$. □

PROOF OF PROPOSITION 1. If the formula Φ begins with $\neg$, there is nothing to prove. Let Φ be represented as $(\Phi_0 \tau \Phi_1)$, where τ is one of the signs $\wedge$, $\vee$ or $\rightarrow$ and Φ_0, Φ_1 are formulas of PC and as $(\Phi_0' \tau' \Phi_1')$, where τ' is one of the signs $\wedge$, $\vee$ or $\rightarrow$ and Φ_0', Φ_1' are formulas of PC. Then Φ_0 is the beginning of Φ_0' or Φ_0' is the beginning of Φ_0. By the lemma $\Phi_0 = \Phi_0'$ and so $\tau = \tau'$ and $\Phi_1 = \Phi_1'$. Hence the representation $\Phi = (\Phi_0 \tau \Phi_1)$ is unique. □

COROLLARY 1. *Let Φ be a formula of PC. Then there is a* 1-1 *correspondence between each occurrence of* (*or* $\neg$ *in* Φ *and some occurrence of a subformula of* Φ *whose first symbol is the occurrence under consideration of* (*or* $\neg$ *respectively.*

PROOF. By the induction on the construction of a formula we can associate with each occurrence of (or $\neg$ *some* such occurrence of a subformula and Lemma 1 allows us to assert the uniqueness of such an occurrence. □

PROPOSITION 2. *If* Φ *is a formula of PC,* η, θ *are occurrences in* Φ *of subformulas* Ψ, X *respectively, then either* η *and* θ *have no occurrences of the symbols of the alphabet of PC in common or one of them is entirely in the other.*

PROOF. If η and θ have any occurrences of symbols in common, then the first occurrence of the first symbol η or θ must be in common. Let the first occurrence of the first symbol η occur in θ. If Ψ is an atomic formula, then the statement is obvious. Let Ψ be nonatomic, then the first symbol of Ψ is (or $\neg$. By Corollary 1 this symbol uniquely defines the occurrence of some subformula Ψ' in X. But this subformula will be a subformula in Φ too. Associated with the occurrence under consideration of (or $\neg$ in Φ is the occurrence η of the subformula Ψ. By virtue of uniqueness, Ψ must coincide with Ψ' and η is entirely in θ. □

If all the occurrences of the subformula Ψ in Φ are replaced by the formula X, then we obtain a new formula which we denote by $(\Phi)^{\Psi}_{X}$. Such a definition is correct, since it follows from Proposition 2 that two distinct occurrences of the subformula Ψ in Φ have no occurrence of the symbols of the alphabet of PC in common.

DEFINITION. *Sequents* of PC are sequences of the following four forms:

$$\Phi_0, \ldots, \Phi_n \vdash \Psi; \quad \Phi_0, \ldots, \Phi_n \vdash; \quad \vdash \Psi; \quad \vdash,$$

where $\Phi_0, \ldots, \Phi_n$ and Ψ are formulas of PC and n is a natural number.

Sequents will often be denoted by $\Gamma \vdash \Psi$ or $\Gamma \vdash$, where Γ denotes a sequence, possibly empty, of formulas of PC.

While formulas of PC may be regarded as "forms" of compound propositions of our language, sequents are "forms" of statements, theorems in which we may clearly distinguish conditions (hypotheses) and conclusion. Namely, regarding $\vdash$ as the sign of (logical) entailment, the sequent $\Phi_0, \ldots, \Phi_n \vdash \Psi$ may be understood to be a statement of the form "(The truth of) the hypotheses $\Phi_0, \ldots, \Phi_n$ (logically) entails the proposition Ψ". Sequents of the form $\Phi_0, \ldots, \Phi_n \vdash$ may be understood to be a statement about joint inconsistency of the hypotheses (conditions) $\Phi_0, \ldots, \Phi_n$.

The rules of inference of PC to be described in the next section reflect (formalize) some simplest standard logical modes of reasoning which allow one to pass from some true statements (theorems) to other true statements (theorems).

Exercises

1. Show that for any word α of the alphabet of PC it is possible to determine in a finite number of steps whether α is a formula of PC or not. (Hint. Use Proposition 1).

2. Replace point 2 in the definition of a formula of PC by the following: if Φ and Ψ are formulas, then $(\Phi) \wedge (\Psi)$, $(\Phi) \vee (\Psi)$, $(\Phi) \to (\Psi')$ and $\neg (\Phi)$ are formulas. Show that with such a definition we have statements similar to Propositions 1 and 2.

3. AXIOM SYSTEM AND RULES OF INFERENCE

Below we shall often deal not with concrete formulas and sequents but with the so-called schemata of formulas and sequents. The letters Φ, Ψ, X (Γ, Δ, θ), possibly with indices from the set of natural numbers, will be called *variables for formulas* (*sequences of formulas*). Let an alphabet *B* contain, besides the symbols of the alphabet of PC, the variables for formulas and sequences of formulas.

A *schema of sequents* (*formulas*) of PC is a word in *B* such that any substitutions in that word of concrete formulas and sequences of concrete formulas for variables of formulas and sequences of formulas, respectively, yield sequents (formulas of PC. The results of such substitutions will be called *instances* of the schema. For example, $\Psi, \Gamma \vdash \Phi \vee \Psi$ and $\Phi \to \to (X_1 \wedge X_2)$ are schemata of sequents and formulas respectively and

$$Q_0 \wedge \neg Q_1, \quad \neg Q_0, \quad \neg (Q_2 \rightarrow Q_1) \vdash Q_3 \vee (Q_0 \wedge \neg Q_1),$$
$$((Q_1 \rightarrow \neg Q_1) \wedge Q_0) \rightarrow (Q_3 \wedge \neg (Q_2 \vee \neg Q_0))$$

are instances of the corresponding schemata *.

DEFINITION. A schema of sequents

$$\Phi \vdash \Phi$$

is called an *axiom schema* of PC. An instance of an axiom schema will be called an *axiom*.

The rules of inference of PC are the following:

1. $\dfrac{\Gamma \vdash \Phi; \Gamma \vdash \Psi}{\Gamma \vdash \Phi \wedge \Psi}$,

2. $\dfrac{\Gamma \vdash \Phi \wedge \Psi}{\Gamma \vdash \Phi}$,

3. $\dfrac{\Gamma \vdash \Phi \wedge \Psi}{\Gamma \vdash \Psi}$,

4. $\dfrac{\Gamma \vdash \Phi}{\Gamma \vdash \Phi \vee \Psi}$,

5. $\dfrac{\Gamma \vdash \Psi}{\Gamma \vdash \Phi \vee \Psi}$,

6. $\dfrac{\Gamma, \Phi \vdash \Psi; \Gamma, X \vdash \Psi; \Gamma \vdash \Phi \vee X}{\Gamma \vdash \Psi}$,

7. $\dfrac{\Gamma, \Phi \vdash \Psi}{\Gamma \vdash \Phi \rightarrow \Psi}$,

8. $\dfrac{\Gamma \vdash \Phi; \Gamma \vdash \Phi \rightarrow \Psi}{\Gamma \vdash \Psi}$,

9. $\dfrac{\Gamma, \neg \Phi \vdash}{\Gamma \vdash \Phi}$,

10. $\dfrac{\Gamma \vdash \Phi; \Gamma \vdash \neg \Phi}{\Gamma \vdash}$,

11. $\dfrac{\Gamma, \Phi, \Psi, \Gamma_1 \vdash X}{\Gamma, \Psi, \Phi, \Gamma_1 \vdash X}$,

12. $\dfrac{\Gamma \vdash \Phi}{\Gamma, \Psi \vdash \Psi}$.

As noted at the end of the preceding section, the rules of inference of PC formalize certain standard logical modes of reasoning. Let us comment at an informal level upon Rules 1 to 12 from this point of view. Rules 1 to 3 are simply rules clarifying the meaning of the word "and" (conjunction). Rules 4, 5 also refer to the clarification of the meaning of the word "or" (disjunction). Rule 6 formalizes the mode of reasoning by "analysis of (two) possible cases". When hypotheses Γ hold, either Φ or X is true. Ψ is true either when conditions Γ and Φ are true or when conditions

---

* When the values of variables for the formulas and sequences of formulas in a schema *C* of sequents (formulas) are fixed in the text the schema *C* is called simply a sequent (a formula).

Γ and X, are true, thus Ψ is always true when hypotheses Γ are satisfied. This is established by considering two possible cases (one of them necessarily holding): (1) conditions Γ and the condition Φ hold; (2) conditions Γ and the condition X hold. Rule 7 formalizes a device of equivalent restatement of a theorem allowing one of the hypothesis of the theorem to be placed into its conclusion in the form of a hypothesis. Rule 8 is one of the logical rules (the rule of modus ponens or detachment) noted already by Aristotle; it shows how to get rid of a hypothesis in the conclusion. Rule 9 formalizes the rule of "arguing by reductio ad absurdum". Suppose that conditions Γ and $\neg\Phi$ can hold simultaneously; coming to a contradiction we conclude that Φ always holds if the conditions Γ hold. Rule 10 is the rule of "discovering (deriving) a contradiction" for a sequence of hypotheses Γ. Rule 11 is of a purely technical formal character: interchange of premises does not affect the truth of the conclusion. Rule 12, sometimes called a "refinement" or the rule of an extra hypothesis, reflects a trivial fact that adding to the hypotheses of a theorem a superfluous hypothesis does not violate the truth of the conclusion of the theorem.

If in the rules of inference we take concrete sequences of formulas of PC as Γ and Γ_1 and concrete formulas as Φ, Ψ, X, then we obtain *instances* (or *applications*) *of the rules of inference.* Rules 1 to 10 are called *basic* and Rules 11 and 12 are *structural.* If Θ is an application of a rule of inference k, then we shall say that the sequent under the line in Θ is obtained from the sequents above the line with the aid of the rule k.

DEFINITION. A *linear proof* in PC is a finite sequence $S_0, \ldots, S_n$ of sequents of PC satisfying the following condition: each sequent S_i, $i \leqslant n$, is either an axiom or obtained from some $S_j, j < i$, using one of the Rules of inference 1 to 12. A sequent S is said to be PC-*provable* or a *theorem* of PC if there is a proof $S_0, \ldots, S_n$ in PC such that $S_n = S$. A formula Φ of PC is said to be PC-*provable* if so is the sequent $\vdash \Phi$.

Notice that if $S_0, \ldots, S_n$ is a proof in PC and $S_0', \ldots, S_k'$ is a proof in PC, then $S_0, \ldots, S_n, S_0', \ldots, S_k'$ is also a proof in PC.

We define inductively the notion of *tree*:

(1) Any sequent is a tree.

(2) If $D_0, \ldots, D_n$ are trees and S is a sequent, then

$$\frac{D_0, \ldots, D_n}{S}$$

is also a tree.

The same sequent may occur in a tree several times. A sequent together with its position in a tree D will be called an *occurrence of the sequent* in the tree D. An occurrence of a sequent in D which has no horizontal line above it will be called an *initial* occurrence in D. An occurrence of a sequent in D which has no horizontal line below it will be called *final* sequent in D. We shall often use the word "sequent" instead of "an occurrence of a sequent" if it is clear from the context what occurrence is meant. It is clear that a tree may have many initial sequents, but there is only one final sequent. The part of a tree consisting of the sequents immediately above the line, below the line and of the line itself is called a *passage*.

DEFINITION. A tree D is said to be a *tree form proof* in PC if all its initial sequents are axioms of PC and its passages are applications of Rules of inference 1 to 12. If S is the final sequent of a tree form proof in D, then D is said to be *tree form proof of S* or a *derivation tree of S* in PC.

Let h be a function defined on the sequents (more precisely, on the occurrences of the sequents) of D and taking as its values natural numbers having the following properties:

(1) $h(S) = 0$ if S is the final sequent of the tree D.

(2) If

$$\frac{S_0, \ldots, S_n}{S}$$

is a passage in D, then $h(S_0) = \ldots = h(S_n) = h(S) + 1$.

It is obvious that conditions (1) and (2) uniquely define the function h. The number $h(S)$ is called the *height* (of the occurrence) *of a sequent S in the tree D*. The maximum height of the sequents occurring in D is called the *height of the tree D*.

PROPOSITION 1. *A sequent S has a tree form proof in PC if and only if S is a theorem of PC.*

PROOF. Let $S_0, \ldots, S_{n-1}, S$ be a linear proof in PC. If S is an axiom, then S will be a tree form proof of the sequent S. Let

$D_0, \ldots, D_{n-1}$ be tree form proofs of the sequents $S_0, \ldots, S_{n-1}$. If $\dfrac{S_{i_1}; \ldots; S_{i_k}}{S}$, $i_1, \ldots, i_k < n$, is the application of some rule, then the tree

$$\frac{D_{i_1}; \ldots; D_{i_k}}{S}$$

will be a tree form proof of the sequent S.

Suppose now that a proof of the sequent S in the form of a tree D is given. We construct a linear proof of S by induction on the height of the sequents in the tree D. The initial sequents in D will be linear proofs. If for all the sequents $S_0, \ldots, S_m$ of height $k + 1$ linear proofs $L_1, \ldots, L_m$ are already constructed, then it is clear that the sequence

$$L_1, \ldots, L_m, S$$

will be a linear proof of a sequent S of height k. ☐

A sequent schema H is said to be PC-*provable* if adding it to PC as an axiom schema does not extend the set of provable sequents. It is clear that this is equivalent to the fact that all instances of the schema H are PC-provable.

Example 1. The following tree shows the provability of the schema $\Phi, \Psi \vdash \Phi \wedge \Psi$ *:

$$\dfrac{\dfrac{\Phi \vdash \Phi}{\Phi, \Psi \vdash \Phi}\ (\text{Rule } 12) \qquad \dfrac{\dfrac{\Psi \vdash \Psi}{\Psi, \Phi \vdash \Psi}\ (\text{Rule } 12)}{\Phi, \Psi \vdash \Psi}\ (\text{Rule } 11)}{\Phi, \Psi \vdash \Phi \wedge \Psi}\ (\text{Rule } 1)$$

A rule of inference is said to be PC-*admissible* if adding it to PC does not extend the set of provable sequents. In particular, Rules 1 to 12 of PC are admissible.

PROPOSITION 2. *The following rules are* PC-*admissible*:

$$\left.\begin{array}{l} \text{(a)}\ \dfrac{\Psi_1, \ldots, \Psi_n \vdash \Phi}{\chi_1, \ldots, \chi_m \vdash \Phi}, \\[2ex] \text{(b)}\ \dfrac{\Psi_1, \ldots, \Psi_n \vdash}{\chi_1, \ldots, \chi_m \vdash} \end{array}\right\} \quad \text{where } \{\Psi_1, \ldots, \Psi_n\} \subseteq \{\chi_1, \ldots, \chi_m\},$$

---

* Instead of "application of Rule 12", etc. we shall write "Rule 12".—*Editor's note.*

$$\text{(c)}\ \frac{\Gamma \vdash \Psi;\ \Gamma, \Psi \vdash \chi}{\Gamma \vdash \chi}, \qquad \text{(g)}\ \frac{\Gamma, \Phi \vdash}{\Gamma \vdash \neg \Phi},$$

$$\text{(d)}\ \frac{\Gamma_1, \Phi, \Psi, \Gamma_2 \vdash \chi}{\Gamma_1, \Phi \wedge \Psi, \Gamma_2 \vdash \chi}, \qquad \text{(h)}\ \frac{\Gamma \vdash \Phi}{\Gamma, \neg \Phi \vdash},$$

$$\text{(e)}\ \frac{\Gamma \vdash \Phi \wedge \neg \Phi}{\Gamma \vdash}, \qquad \text{(i)}\ \frac{\Gamma, \Phi \vdash \Psi}{\Gamma, \neg \Psi \vdash \neg \Phi},$$

$$\text{(f)}\ \frac{\Gamma \vdash}{\Gamma \vdash \Psi}, \qquad \text{(j)}\ \frac{\Gamma, \neg \Phi \vdash \neg \Psi}{\Gamma, \Psi \vdash \Phi},$$

PROOF. Before proving that rule (a) is admissible we establish the admissibility of an instance of it:

$$\text{(a}'\text{)}\ \frac{\Gamma_1, \Phi, \Phi, \Gamma_2 \vdash \Psi}{\Gamma_1, \Phi, \Gamma_2 \vdash \Psi}.$$

Applying Rule 11 several times changes the sequent Γ_1, Φ, Φ, $\Gamma_2 \vdash \Psi$ into $\Gamma_1, \Phi, \Gamma_2, \Phi \vdash \Psi$. Using Rule 12 we can obtain from the axiom $\Phi \vdash \Phi$ a sequent $\Gamma_1, \Phi, \Gamma_2 \vdash \Phi$. The tree

$$\frac{\dfrac{\Gamma_1, \Phi, \Gamma_2, \Phi \vdash \Psi}{\Gamma_1, \Phi, \Gamma_2 \vdash \Phi \to \Psi} \quad \Gamma_1, \Phi, \Gamma_2 \vdash \Phi}{\Gamma_1, \Phi, \Gamma_2 \vdash \Psi}$$

establishes (a′). It is clear that the admissibility of (a) follows from that of (a′) and Rules 11 and 12.

The admissibility of (b) follows from that of rules (a), (e) and (f). The admissibility of (c) is demonstrated by the following tree

$$\frac{\dfrac{\Gamma, \Psi \vdash \chi}{\Gamma \vdash \Psi \to \chi};\ \Gamma \vdash \Psi}{\Gamma \vdash \chi}.$$

In addition we show the admissibility of (f) and (g), leaving the other rules as an exercise to the reader.

It is clear that the sequent $\Gamma \vdash$ can be obtained only by Rule 10. Therefore, if $\Gamma \vdash$ is provable, then so are the sequents $\Gamma \vdash \Phi_0$ and $\Gamma \vdash \neg \Phi_0$ for some formula Φ_0. To prove the admissibility of a rule of the form

$$\frac{\Gamma \vdash}{S}$$

it suffices to construct a tree whose initial sequents are either provable schemata of $\Gamma \vdash \Phi_0$ and $\Gamma \vdash \neg \Phi_0$ whose final sequent is the sequent S and whose passages are Rules 1 to 12.

$$(f)\ \dfrac{\dfrac{\dfrac{\Gamma \vdash \Phi_0}{\Gamma, \neg \Psi \vdash \Phi_0} \qquad \dfrac{\Gamma \vdash \neg \Phi_0}{\Gamma, \neg \Psi \vdash \neg \Phi_0}}{\Gamma, \neg \Psi \vdash}}{\Gamma \vdash \Psi}.$$

(g) We use the provability of the schema $\Gamma, \neg \Psi$, and $\Psi \vdash$ and leave it to the reader as an exercise.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, \Phi \vdash \Phi_0}{\Gamma, \Phi, \neg\neg\Phi \vdash \Phi_0}}{\Gamma, \neg\neg\Phi, \Phi \vdash \Phi_0}}{\Gamma, \neg\neg\Phi \vdash \Phi \to \Phi_0}; \quad \dfrac{\Gamma, \neg\neg\Phi, \neg\Phi \vdash}{\Gamma, \neg\neg\Phi \vdash \Phi}}{\Gamma, \neg\neg \vdash \Phi_0} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\Gamma, \Phi \vdash \neg\Phi_0}{\Gamma, \Phi, \neg\neg\Phi \vdash \neg\Phi_0}}{\Gamma, \neg\neg\Phi, \Phi \vdash \neg\Phi_0}}{\Gamma, \neg\neg\Phi \vdash \Phi \to \neg\Phi_0} \quad \dfrac{\Gamma, \neg\neg\Phi, \neg\Phi \vdash}{\Gamma, \neg\neg\Phi \vdash \Phi}}{\Gamma, \neg\neg\Phi \vdash \neg\Phi_0}}{\Gamma, \neg\neg\Phi \vdash}}{\Gamma \vdash \neg\Phi} \quad \square$$

A finite sequence of sequents $S_0, \ldots, S_n$ is said to be the *quasi-derivation of the sequent S_n in PC* if each sequent occurring in it is PC-provable or can be obtained from the preceding sequents by a PC-admissible rule of inference. A tree D is said to be a *tree form quasi-derivation of a sequent S in PC* if any initial sequent of D is PC-provable, the final sequence is S and the passages are PC-admissible rules of inference.

It is obvious that any sequent for which there is a quasi-derivation or a tree form quasi-derivation is provable.

EXAMPLE 2. We prove the sequent $\vdash Q_0 \vee \neg Q_0$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\neg Q_0 \vdash \neg Q_0}{\neg Q_0 \vdash Q_0 \vee \neg Q_0}; \quad \neg(Q_0 \vee \neg Q_0) \vdash \neg(Q_0 \vee \neg Q_0)}{\neg(Q_0 \vee \neg Q_0), \neg Q_0 \vdash}}{\neg(Q_0 \vee \neg Q_0) \vdash Q_0}}{\neg(Q_0 \vee \neg Q_0) \vdash Q_0 \vee \neg Q_0}; \quad \neg(Q_0 \vee \neg Q_0) \vdash \neg(Q_0 \vee \neg Q_0)}{\neg(Q_0 \vee \neg Q_0) \vdash}}{\vdash Q_0 \vee \neg Q_0}.$$

Notice that the above tree is not a PC proof, since the second passage is not an application of any of the rules. It is clear, however, that we can obtain a proof by adding to this tree application of Rules 11 and 12. In what follows, unless otherwise specified, we shall use admissible rules that can be obtained from the basic rules by combining them with structural rules, as the following:

$$\frac{\Phi_1, \ldots, \Phi_n, \Phi \vdash \Psi;\ \Psi_1, \ldots, \Psi_m, \mathrm{X} \vdash \Psi;\ \mathrm{X}_1, \ldots, \mathrm{X}_k \vdash \Phi \vee \mathrm{X}}{\Phi_{n+1}, \ldots, \Phi_{n+r} \vdash \Psi},$$

where $\{\Phi_1, \ldots, \Phi_n, \Psi_1, \ldots, \Psi_m, \mathrm{X}_1, \ldots, \mathrm{X}_k\} \subseteq \{\Phi_{n+1}, \ldots, \Phi_{n+r}\}$.

Exercises

1. Establish PC-provability of the following schemata:
(a) $\Gamma_1, \Phi, \Gamma_2 \vdash \Phi$; (b) $\Gamma, \neg\Phi, \Phi \vdash$;
(c) $\Phi \wedge \Psi \vdash \Psi \wedge \Phi$; (d) $\Phi \vee \Psi \vdash \Psi \vee \Phi$.
2. Prove the PC-admissibility of rules:

$$\text{(k)}\ \frac{\Gamma, \Phi \vdash \Psi}{\Gamma, \neg\Psi \vdash \neg\Phi}, \qquad \text{(l)}\ \frac{\Gamma, \Phi \vdash \neg\Psi}{\Gamma, \Psi \vdash \neg\Phi}.$$

4. THE EQUIVALENCE OF FORMULAS

Denote by F the set of all formulas of PC. Let $s\colon F \to F$ be a mapping of F into F satisfying the conditions:

$$(1)\ s(\Phi \to \Psi) = (s(\Phi) \to s(\Psi)),$$

$$(2)\ s(\Phi \wedge \Psi) = (s(\Phi) \wedge s(\Psi)),$$

$$(3)\ s(\Phi \vee \Psi) = (s(\Phi) \vee s(\Psi)),$$

$$(4)\ s(\neg\Phi) = \neg s(\Phi).$$

Any such mapping will be called a *substitution*. The reader may see for himself that any substitution is uniquely defined by its values of atomic formulas, i. e. if $P_0, \ldots, P_n$ are all atomic subformulas of a formula Φ and s_0 and s_1 are substitutions such that $s_0(P_i) = s_1(P_i)$ for $i \leqslant n$, then $s_0(\Phi) = s_1(\Phi)$. For the result of a substitution $s(\Phi)$, we introduce the notation $s(\Phi) = (\Phi)^{P_0, \ldots, P_n}_{s(P_0), \ldots, s(P_n)}$ which agrees with the notation $(\Phi)^{\Psi}_{\mathrm{X}}$ introduced in Section 2.

We extend the mapping s to include sequents:

(5) $s(\Phi_1, \ldots, \Phi_n \vdash \Psi) = s(\Phi_1), \ldots, s(\Phi_n) \vdash s(\Psi)$; $s(\Phi_1, \ldots$ $\ldots, \Phi_n \vdash) = s(\Phi_1), \ldots, s(\Phi_n) \vdash$; $s(\vdash \Phi) = \vdash s(\Phi)$; $s(\vdash) = \vdash$.

It is possible to define by induction the extension of s to trees:

(6) $s\left(\dfrac{D_1; \ldots; D_k}{S}\right) = \dfrac{s(D_1); \ldots; s(D_k)}{s(S)}$.

THEOREM 1 (Substitution). *Let a mapping* $s\colon F \to F$ *satisfy conditions* (1) *to* (6) *and let* S *be a PC-provable sequent. Then the sequent* $s(S)$ *is PC-provable.*

PROOF. We shall prove by induction of the height of a tree that if D is a tree form proof of the sequent S in PC, then $s(D)$ is a proof of the sequent $s(S)$ in PC. If S is an axiom, then $s(S)$ is also an axiom. Let

$$D = \cfrac{\cfrac{D_0^0; \ldots; D_{i0}^0}{S_0} \;\ldots\; \cfrac{D_0^k; \ldots; D_{ik}^k}{S_k}}{S},$$

then

$$s(D) = \cfrac{\cfrac{s(D_0^0); \ldots; s(D_{i0}^0)}{s(S_0)} \;\ldots\; \cfrac{s(D_0^k); \ldots; s(D_{ik}^k)}{s(S_k)}}{s(S)},$$

By virtue of the induction hypothesis it suffices to prove that in the tree $s(D)$ the last passage is an application of the same rule as in the last passage of the tree D. But this is obvious, since properties (1) to (5) ensure that the passages are preserved. For example, if

$$\frac{\Phi_0, \Phi \vdash \Psi;\ \Phi_0, \mathrm{X} \vdash \Psi;\ \Phi_0 \vdash \Phi \vee \mathrm{X}}{\Phi_0 \vdash \Psi}$$

is the last passage in the tree D, then

$$\frac{s(\Phi_0), s(\Phi) \vdash s(\Psi);\ s(\Phi_0), s(\mathrm{X}) \vdash s(\Psi);\ s(\Phi_0) \vdash s(\Phi) \vee s(\mathrm{X})}{s(\Phi_0) \vdash s(\Psi)}$$

is an application of Rule 4 and the last passage in the tree $s(D)$. □

In other words, the substitution theorem states that if in a provable sequent we substitute arbitrary formulas for the propositional variables, then the resulting sequent will be provable.

DEFINITION. Two formulas Φ and Ψ are said to be *equivalent* (designated $\Phi \equiv \Psi$) if two sequents $\Phi \vdash \Psi$ and $\Psi \vdash \Phi$ are PC-provable.

Notice that "$\equiv$" is the symbol of the language in which we prove statements about the calculus but not the symbol of the propositional calculus. This language is sometimes called *metalanguage.* The concepts of schema and proof are also metalanguage concepts.

LEMMA 1. *The relation* $\Phi \equiv \Psi$ *is an equivalence relation, i. e. for any formulas* Φ, Ψ, X *of PC the following statements are true*:

(a) $\Phi \equiv \Phi$;

(b) *if* $\Phi \equiv \Psi$, *then* $\Psi = \Phi$;

(c) *if* $\Phi \equiv \Psi$ *and* $\Psi \equiv X$, *then* $\Phi \equiv X$.

PROOF. (a) follows from the fact that $\Phi \vdash \Phi$ is an axiom. (b) follows from the symmetry of Φ and Ψ in the definition of the relation $\Phi \equiv \Psi$. If $\Phi \vdash \Psi$ and $\Psi \vdash X$ are provable, then by Proposition 3.2 (c) $\Phi \vdash X$ is provable. Similarly, if $X \vdash \Psi$, $\Psi \vdash \Phi$ are provable, then $X \vdash \Phi$ is provable. □

LEMMA 2. (a) *If* $\Phi \equiv \Psi$, *then* Φ *is PC-provable if and only if* Ψ *is PC-provable.*

(b) *If* $\Phi_1 \equiv \Psi_1$, *and* $\Phi_2 \equiv \Psi_2$, *then* $(\Phi_1 \wedge \Phi_2) \equiv (\Psi_1 \wedge \Psi_2)$, $(\Phi_1 \vee \Phi_2) \equiv (\Psi_1 \vee \Psi_2)$, $(\Phi_1 \to \Phi_2) \equiv (\Psi_1 \to \Psi_2)$ *and* $\neg\Phi_1 \equiv \neg\Psi_1$.

PROOF. If $\vdash \Phi$ and $\Phi \vdash \Psi$ are provable, then the tree

$$\frac{\dfrac{\Phi \vdash \Psi}{\vdash \Phi \to \Psi}; \ \vdash \Phi}{\vdash \Psi}$$

will be a quasi-derivation of $\vdash \Psi$. Similarly from the provability of $\vdash \Psi$ and $\Psi \vdash \Phi$ we obtain the provability of $\vdash \Phi$. Statement (a) is thus proved.

By virtue of the symmetry of Φ_i and Ψ_i in (b) it suffices to prove the sequents $\neg\Phi_1 \vdash \neg\Psi_1$, $\Phi_1 \wedge \Phi_2 \vdash \Psi_1 \wedge \Psi_2$, $\Phi_1 \vee \Phi_2 \vdash \Psi_1 \vee \Phi_2$ and $\Phi_1 \to \Phi_2 \vdash \Psi_1 \to \Psi_2$. The following four quasi-derivations complete the proof:

$$(1)\ \frac{\dfrac{\Psi_1 \vdash \Phi_1, \ \neg\Phi_1 \vdash \neg\Phi_1}{\Psi_1, \neg\Phi_1 \vdash}}{\neg\Phi_1 \vdash \neg\Psi_1}$$

$$(2)\ \dfrac{\dfrac{\Phi_1 \wedge \Phi_2 \vdash \Phi_1;\ \Phi_1 \vdash \Psi_1}{\Phi_1 \wedge \Phi_2 \vdash \Psi_1} \qquad \dfrac{\Phi_1 \wedge \Phi_2 \vdash \Phi_2;\ \Phi_2 \vdash \Psi_2}{\Phi_1 \wedge \Phi_2 \vdash \Psi_2}}{\Phi_1 \wedge \Phi_2 \vdash \Psi_1 \wedge \Psi_2}$$

$$(3)\ \dfrac{\dfrac{\Phi_1 \vdash \Psi_1}{\Phi_1 \vdash \Psi_1 \vee \Psi_2} \quad \dfrac{\Phi_2 \vdash \Psi_2}{\Phi_2 \vdash \Psi_1 \vee \Psi_2} \quad \Phi_1 \vee \Phi_2 \vdash \Phi_1 \vee \Phi_2}{\Phi_1 \vee \Phi_2 \vdash \Psi_1 \vee \Psi_2}$$

$$(4)\ \dfrac{\dfrac{\dfrac{\Psi_1 \vdash \Phi_1;\ \Phi_1 \to \Phi_2 \vdash \Phi_1 \to \Phi_2}{\Phi_1 \to \Phi_2, \Psi_1 \vdash \Phi_2} \quad \dfrac{\Phi_2 \vdash \Psi_2}{\vdash \Phi_2 \to \Psi_2}}{\Phi_1 \to \Phi_2, \Psi_1 \vdash \Psi_2}}{\Phi_1 \to \Phi_2 \vdash \Psi_1 \to \Psi_2}\ . \ \square$$

THEOREM 2 (Replacement). *Let Φ be a formula of PC and let Ψ be its subformula. Suppose Φ' is obtained from Φ by replacing some occurrence of Ψ by a formula Ψ'. In this case, if $\Psi \equiv \Psi'$, then $\Phi \equiv \Phi'$.*

PROOF. If $\Psi = \Phi$, then the theorem is trivial. Further we proceed by induction on the length of Φ. If $\Phi = Q_i$, then $\Psi = \Phi$.

Four cases are possible for the induction step:

(a) $\Phi = \Phi_1 \wedge \Phi_2$; (b) $\Phi = \Phi_1 \vee \Phi_2$;

(c) $\Phi = \Phi_1 \to \Phi_2$; (d) $\Phi = \neg \Phi_1$.

By Proposition 2.2 any occurrence of $\Psi \neq \Phi$ is contained either in Φ_1 or in Φ_2, therefore the equivalence $\Phi \equiv \Phi'$ follows from the induction hypothesis and Lemma 2(b). $\square$

Exercises

1. Suppose formulas Φ and Ψ of PC contain only one propositional variable, P, and for some substitutions s_1 and s_2 we have $s_1(\Phi) = \Psi$ and $s_2(\Psi) = \Phi$. Show that $\Phi = \Psi$.

2. Suppose $\Phi \equiv \Psi$ and there is a propositional variable P occurring in both Φ and Ψ. Show that there is a formula X equivalent to the formulas Φ and Ψ, all propositional variables of which are contained in both Φ and Ψ. (*Hint.* Use Theorem 1.)

5. NORMAL FORMS

The notion of the equivalence of formulas of PC will be of great importance to us, since the basic properties under study of the formulas of PC are preserved when we pass to equivalent formulas. It is very important therefore to be able to find for each formula of PC its equivalent but constructed as simple as possible. In this section we shall define such "canonical" representatives for the formulas of PC.

LEMMA 1. Let Φ and Ψ be formulas of PC. Then we have the following equivalences:

(a) $(\Phi \to \Psi) \equiv (\neg \Phi \vee \Psi)$;
(b) $\neg \neg \Phi \equiv \Phi$;
(c) $\neg(\Phi \wedge \Psi) \equiv (\neg \Phi \vee \neg \Psi)$;
(d) $\neg(\Phi \vee \Psi) \equiv (\neg \Phi \wedge \neg \Psi)$;
(e) $\Phi \equiv (\Phi \vee \Phi)$;
(f) $\Phi \equiv (\Phi \wedge \Phi)$.

PROOF. We give quasi-derivations for statement (a):

$$\frac{\dfrac{\dfrac{\Phi \vdash \Phi;\ \Phi \to \Psi \vdash \Phi \to \Psi}{\Phi \to \Psi, \Phi \vdash \Psi}}{\Phi \to \Psi, \Phi \vdash \neg \Phi \vee \Psi};\ \dfrac{\neg \Phi \vdash \neg \Phi}{\neg \Phi \vdash \neg \Phi \vee \Psi};\ \vdash \Phi \vee \neg \Phi}{\Phi \to \Psi \vdash \neg \Phi \vee \Psi};$$

$$\frac{\dfrac{\dfrac{\Phi \vdash \Phi;\ \neg \Phi \vdash \neg \Phi}{\Phi, \neg \Phi \vdash}}{\Phi, \neg \Phi \vdash \Psi};\quad \Psi \vdash \Psi;\ \neg \Phi \vee \Psi \vdash \neg \Phi \vee \Psi}{\dfrac{\neg \Phi \vee \Psi, \Phi \vdash \Psi}{\neg \Phi \vee \Psi \vdash \Phi \to \Psi}}.$$

Notice that the provability of $\vdash \Phi \vee \neg \Phi$ follows from Example 3.2 and the substitution theorem.

The proof of the remaining statements of Lemma 1 is left to the reader. □

LEMMA 2. *Any formula Φ of the propositional calculus is equivalent to a formula Ψ containing no implication sign.*

PROOF. We define the mapping $\alpha: F \to F$ by induction on the length of a formula:

(1) $\alpha(Q_i) = Q_i$,
(2) $\alpha(\Phi \wedge \Psi) = \alpha(\Phi) \wedge \alpha(\Psi)$,
(3) $\alpha(\Phi \vee \Psi) = \alpha(\Phi) \vee \alpha(\Psi)$,
(4) $\alpha(\neg \Phi) = \neg \alpha(\Phi)$,
(5) $\alpha(\Phi \to \Psi) = \neg \alpha(\Phi) \vee \alpha(\Psi)$.

Then $\alpha(\Phi)$ contains no implication sign and $\alpha(\Phi) \equiv \Phi$ follows by induction from Lemma 4.2(b) and Lemma 1(a). □

LEMMA 3. *Any formula Φ of PC is equivalent to a formula Ψ without the implication sign such that there are negation signs only in front of atomic subformulas.*

PROOF. Let F^{-} be a set of formulas containing no implication sign. We define the mapping β: $F^{-} \to F^{-}$ by induction:

(1) $\beta(Q_i) = Q_i$,

(2) $\beta(\neg Q_i) = \neg Q_i$,

(3) $\beta(\Phi \wedge \Psi) = \beta(\Phi) \wedge \beta(\Psi)$,

(4) $\beta(\Phi \vee \Psi) = \beta(\Phi) \vee \beta(\Psi)$,

(5) $\beta(\neg(\Phi \wedge \Psi)) = \beta(\neg \Phi) \vee \beta(\neg \Psi)$,

(6) $\beta(\neg(\Phi \vee \Psi)) = \beta(\neg \Phi) \wedge \beta(\neg \Psi)$,

(7) $\beta(\neg \neg \Phi) = \beta(\Phi)$.

Let $X = \alpha(\Phi)$, where α is the mapping of Lemma 2. The equivalence $X \equiv \beta(X)$ is easy to obtain by induction on the length of X using Lemma 1 and Lemma 4.2(b). It is obvious that $\Psi = \beta(X)$ satisfies the requirements of Lemma 3. □

LEMMA 4. *Let Φ, Ψ, and X be formulas of PC. Then*

(a) $(\Phi \wedge \Psi) \equiv (\Psi \wedge \Phi)$;

(a′) $(\Phi \vee \Psi) \equiv (\Psi \vee \Phi)$;

(b) $((\Phi \wedge \Psi) \wedge X) \equiv (\Phi \wedge (\Psi \wedge X))$;

(b′) $((\Phi \vee \Psi) \vee X) \equiv (\Phi \vee (\Psi \vee X))$;

(c) $(\Phi \wedge (\Psi \vee X)) \equiv ((\Phi \wedge \Psi) \vee (\Phi \wedge X))$;

(c′) $(\Phi \vee (\Psi \wedge X)) \equiv ((\Phi \vee \Psi) \wedge (\Phi \vee X))$.

PROOF. To avoid overloading the presentation we prove only (c). The remaining equivalences the reader will easily prove himself using the experience acquired while analyzing the proofs given earlier.

$$\dfrac{\dfrac{\dfrac{\Phi \wedge (\Psi \vee X) \vdash \Phi;\ \Psi \vdash \Psi}{\Phi \wedge (\Psi \vee X), \Psi \vdash \Phi \wedge \Psi}}{\Phi \wedge (\Psi \vee X), \Psi \vdash (\Phi \wedge \Psi) \vee (\Phi \wedge X)};\ \dfrac{\dfrac{\Phi \wedge (\Psi \vee X) \vdash \Phi;\ X \vdash X}{\Phi \wedge (\Psi \vee X), X \vdash \Phi \wedge X}}{\Phi \wedge (\Psi \vee X), X \vdash (\Phi \wedge \Psi) \vee (\Phi \wedge X)};\ \Phi \wedge (\Psi \vee X), \vdash \Psi \vee X)}{\Phi \wedge (\Psi \wedge X) \vdash (\Phi \wedge \Psi) \vee (\Phi \wedge X)};$$

$$\dfrac{\dfrac{\dfrac{\Phi \wedge \Psi \vdash \Psi}{\Phi \wedge \Psi \vdash \Psi \vee X};\ \Phi \wedge \Psi \vdash \Phi}{\Phi \wedge \Psi \vdash \Phi \wedge (\Psi \vee X)};\quad \dfrac{\Phi \wedge X \vdash \Phi;\ \dfrac{\Phi \wedge X \vdash X}{\Phi \wedge X \vdash \Psi \vee X}}{\Phi \wedge X \vdash \Phi \wedge (\Psi \vee X)};\quad (\Phi \wedge \Psi) \vee (\Phi \wedge X) \vdash (\Phi \wedge \Psi) \vee (\Phi \wedge X)}{(\Phi \wedge \Psi) \vee (\Phi \wedge X) \vdash \Phi \wedge (\Psi \vee X)} \quad \square$$

Now we define the important notions of *disjunctive* and *conjunctive* terms of a formula. For any formula Φ we denote the set of all disjunctive terms of Φ by $D(\Phi)$ and the set of all conjunctive terms of Φ by $K(\Phi)$, which we define by induction on the length of Φ.

(a) If Φ is not representable as a disjunction, i. e. as $\Phi = (\Phi_0 \vee \Phi_1)$, then $D(\Phi) = \{\Phi\}$, i. e. Φ is its only disjunctive term.

(b) If $\Phi = (\Phi_0 \vee \Phi_1)$, then $D(\Phi) = D(\Phi_0) \cup D(\Phi_1)$.

The set $K(\Phi)$ is defined dually. (a) If Φ does not have the form $\Phi_0 \wedge \Phi_1$, then $K(\Phi) = \{\Phi\}$; (b) if $\Phi = \Phi_0 \wedge \Phi_1$, then $K(\Phi) = K(\Phi_0) \cup K(\Phi_1)$.

PROPOSITION 1. *Let Φ and Ψ be formulas of PC. If $D(\Phi) \subseteq D(\Psi)$, then the sequent $\Phi \vdash \Psi$ is PC-provable.*

PROOF. By induction on the number of disjunctive terms in Φ, i. e. on the number $|D(\Phi)|$ of elements in the set $D(\Phi)$.

Let $|D(\Phi)| = 1$, i. e. $D(\Phi) = \{\Phi_0\}$. We establish by induction on the length of Φ that in this case $\Phi \equiv \Phi_0$. Indeed, if $\Phi = \Phi_0$, then this is obvious. If $\Phi = \Phi' \vee \Phi''$, then $D(\Phi') = D(\Phi'') = D(\Phi) = \{\Phi_0\}$ and by the induction hypothesis $\Phi' \equiv \Phi_0$, $\Phi'' \equiv \Phi_0$. By Lemma 4.2(b) $\Phi' \vee \Phi'' \equiv \Phi_0 \vee \Phi_0$ and by Lemma 1(e) $\Phi_0 \vee \Phi_0 \equiv \Phi_0$, hence $\Phi = (\Phi' \vee \Phi'') \equiv \Phi_0$.

We now show by induction on the length of Ψ that if $\Phi_0 \in D(\Psi)$, then the sequent $\Phi_0 \vdash \Psi$ is provable. If Ψ has no form $\Psi_0 \vee \Psi_1$, then $D(\Psi) = \{\Psi\}$, hence $\Phi_0 = \Psi$ and $\Phi_0 \vdash \Psi$ is an axiom. Let $\Psi = \Psi_0 \vee \Psi_1$, then $D(\Psi) = D(\Psi_0) \cup D(\Psi_1)$ and Φ_0 is in $D(\Psi_0)$ or $D(\Psi_1)$. Let $\Phi_0 \in D(\Psi_i)$, $i \leqslant 1$. By the induction hypothesis $\Phi_0 \vdash \Psi_i$ is provable, hence

$$\frac{\Phi_0 \vdash \Psi_i}{\Phi_0 \vdash \Psi_0 \vee \Psi_i}$$

is a quasi-derivation of the sequent $\Phi_0 \vdash \Psi$. Together with the equivalence $\Phi \equiv \Phi_0$, this shows that in the case $|D(\Phi)| = 1$ the sequent $\Phi \vdash \Psi$ is provable.

Now suppose that $|D(\Phi)| = n > 1$ and for any formulas Φ', Ψ' such that $|D(\Phi')| < n$ and $D(\Phi') \subseteq D(\Psi')$ the sequent $\Phi' \vdash \Psi'$ is provable. The statement will be proved by induction on the length of Φ. If Φ is of minimal length among formulas Φ' such that $D(\Phi') = D(\Phi)$, then $\Phi = (\Phi_0 \vee \Phi_1)$, $|D(\Phi_0)| < n$, $|D(\Phi_1)| < n$ and by the induction hypothesis it follows from

$D(\Phi_i) \subseteq D(\Phi) \subseteq D(\Psi)$ that the sequents $\Phi_0 \vdash \Psi$, $\Phi_1 \vdash \Psi$ are provable. Then

$$\frac{\Phi_0 \vdash \Psi;\ \Phi_1 \vdash \Psi;\ \Phi \vdash \Phi_0 \vee \Phi_1}{\Phi \vdash \Psi}$$

is a quasi-derivation of the required sequent. The same reasoning completes the proof. If $\Phi = \Phi_0 \vee \Phi_1$, then for Φ_i, $i \leqslant 1$, either $|D(\Phi_i)| < n$ or $|D(\Phi_i)| = n$ and the length of Φ_i is smaller than that of Φ; in any case the sequents $\Phi_0 \vdash \Psi$ and $\Phi_1 \vdash \Psi$ are provable by the induction hypotheses and hence so is the sequent $\Phi \vdash \Psi$. □

COROLLARY 1. *If* $D(\Phi) = D(\Psi)$, *then* $\Phi \equiv \Psi$. □

The corollary obtained shows that up to the equivalence of formulas it is possible to use the notation $\bigvee\limits_{i=1}^{n} \Phi_i$ or $\Phi_1 \vee \ldots \vee \Phi_n$ for formulas Φ such that $D(\Phi) = \{\Phi_1, \ldots, \Phi_n\}$.

For conjunctive terms the situation is quite similar. The proof of the following proposition is left to the reader.

PROPOSITION 2. *Let* Φ *and* Ψ *be formulas of PC.* If $K(\Psi) \subseteq K(\Phi)$, *then the sequent* $\Phi \vdash \Psi$ *is provable.* □

COROLLARY 2. *If* $K(\Phi) = K(\Psi)$, then $\Phi \equiv \Psi$. □

This allows us to use generalized notation of the form $\bigwedge\limits_{i=1}^{n} \Phi_i$ or $\Phi_1 \wedge \ldots \wedge \Phi_n$ for all formulas Φ such that $K(\Phi) = \{\Phi_1, \ldots, \Phi_n\}$.

LEMMA 5. *For any finite sequence* Γ *and any formula* Φ *the sequent* $\Gamma \vdash \Phi$ *is provable if and only if sequents* $\Gamma \vdash \Phi'$ *are provable for all* $\Phi' \in K(\Phi)$.

PROOF. In one direction the lemma follows from Proposition 2. Suppose that for any $\Phi' \in K(\Phi)$ the sequent $\Gamma \vdash \Phi'$ is provable. We show by induction on the length of Φ that $\Gamma \vdash \Phi$ is provable. If Φ is not representable as $\Phi_0 \wedge \Phi_1$, then there is nothing to prove. If $\Phi = \Phi_0 \wedge \Phi_1$, then by the induction hypothesis $\Gamma \vdash \Phi_0$ and $\Gamma \vdash \Phi_1$ are provable (since $K(\Phi_i) \subseteq K(\Phi)$). Hence

$$\frac{\Gamma \vdash \Phi_0;\ \Gamma \vdash \Phi_1}{\Gamma \vdash \Phi_0 \wedge \Phi_1}$$

is a quasi-derivation of the sequent $\Gamma \vdash \Phi$. □

DEFINITION. We shall say that Φ is an *elementary disjunction* if each disjunctive term of Φ is either an atomic formula or the negation of an atomic formula. We shall say that Φ is in *conjunctive normal form (cnf)* if each conjunctive term of Φ is an elementary disjunction. A formula Φ in conjunctive normal form can be written up to equivalence as $\bigwedge_{i=0}^{n} (\Phi_0^i \vee \ldots \vee \Phi_{m_i}^i)$ where formulas Φ_j^i are atomic formulas or the negations of atomic formulas and $\Phi_0^i \vee \ldots \vee \Phi_{m_i}^i$ are generalized symbols for conjunctive terms of Φ.

Defined dually (i. e. by replacing $\wedge$ by $\vee$ and $\vee$ by $\wedge$) are the notions of *elementary conjunction* and *disjunctive normal form (dnf)*.

THEOREM 3. *For any formula Φ of PC there is an equivalent formula Ψ in cnf.*

PROOF. Let Ψ_1 be a formula equivalent to Φ, containing no implication sign and with all of its negation signs preceding atomic subformulas. We shall prove the theorem by induction on the length of Ψ_1. If Ψ_1 is an atomic formula or its negation, then Ψ_1 is already in cnf. If $\Psi_1 = \Phi_1 \wedge \Phi_2$ and X_1 and X_2 are the formulas which are equivalent to Φ_1, and Φ_2, in cnf respectively, then it is obvious that the formula $X_1 \wedge X_2$ is equivalent to Ψ_1 and is in cnf.

Let $\Psi_1 = \Phi_1 \vee \Phi_2$. Let X_1 and X_2 be in cnf, $X_1 \equiv \Phi_1$ and $X_2 \equiv \Phi_2$. By the replacement theorem $\Psi_1 \equiv X_1 \vee X_2$. We shall prove the fact that $X_1 \vee X_1$ is equivalent to some Ψ in cnf by induction on $n = m_1 + m_2$, where m_i is the number of signs $\wedge$ in X_i, $i = 1, 2$. If $m_1 = m_2 = 0$, then $X_1 \vee X_2$ being an elementary disjunction is in cnf. Suppose, for example, that m_2 is nonzero. Then $X_2 = X_3 \wedge X_4$. By Lemma 4(c′) we get

$$X_1 \vee X_2 = X_1 \vee (X_3 \wedge X_4) \equiv (X_1 \vee X_3) \wedge (X_1 \vee X_4).$$

By the induction hypothesis $X_1 \vee X_3$ and $X_1 \vee X_4$ are equivalent to Ψ_2 and, respectively, to Ψ_3, which are in cnf. It is clear that $\Psi = \Psi_2 \wedge \Psi_3$ satisfies the requirements of the theorem. ☐

The proof of the next theorem is similar to that of Theorem 3 and is left to the reader.

THEOREM 4. *For any formula* Φ *of PC there is a formula* Ψ *that is equivalent to it and is in dnf.* □

DEFINITION. We shall say that a formula Φ of PC is in *principal cnf* (*dnf*) if the following conditions hold:

(1) Φ is in cnf (dnf);

(2) any propositional variable P occurring in Φ has in any conjunctive (disjunctive) term of Φ exactly one occurrence;

(3) any two distinct occurrences of conjunctive (disjunctive) terms of Φ have distinct sets of disjunctive (conjunctive) terms.

For example, of the formulas

$$(Q_1 \vee Q_3) \vee \neg Q_0, \quad (Q_2 \wedge Q_4) \vee (Q_4 \wedge Q_2), \quad (Q_1 \wedge \neg Q_2) \vee (Q_2 \wedge \neg Q_1)$$

in dnf the first is in principal cnf and the third is in principal dnf; the first and second formulas are not in principal dnf. (Why?)

THEOREM 5. *If a formula* Φ *of PC is not PC-provable, then there is an equivalent formula* Ψ *which is in principal cnf.*

We first prove three auxiliary statements.

LEMMA 6. *If for some formula* Φ *of PC there is a formula* Ψ *such that* $\Psi, \neg\Psi \in D(\Phi)$, *then* Φ *is provable.*

PROOF. Indeed, the formula $\Psi \vee \neg\Psi$ is provable and $D(\Psi \vee \neg\Psi) \subseteq D(\Phi)$. By Proposition 1 $\Psi \vee \neg\Psi \vdash \Phi$ is a provable sequent, but then Φ is a provable formula. □

LEMMA 7. *If* Φ *is a PC-provable formula, then* $\Phi \wedge \Psi \equiv \Psi$ *for any formula* Ψ *of PC.*

PROOF. The following trees are quasi-derivations of the required sequents:

$$\frac{\Phi \wedge \Psi \vdash \Phi \wedge \Psi}{\Phi \wedge \Psi \vdash \Psi}, \qquad \frac{\vdash \Phi;\ \Psi \vdash \Psi}{\Psi \vdash \Phi \wedge \Psi}. \ \Box$$

LEMMA 8. *For any formulas* Φ *and* Ψ *of PC we have the equivalence* $\Phi \equiv \Phi \vee (\Psi \wedge \neg\Psi)$.

PROOF. The following quasi-derivations establish the provability of the required sequents

$$\frac{\Phi \vdash \Phi}{\Phi \vdash \Phi \vee (\Psi \wedge \neg\Psi)},$$

$$\frac{\Phi \vdash \Phi;\ \dfrac{\dfrac{\Psi \wedge \neg\Psi \vdash \Psi;\ \Psi \wedge \neg\Psi \vdash \neg\Psi}{\Psi \wedge \neg\Psi \vdash}}{\Psi \wedge \neg\Psi \vdash \Phi};\ \Phi \vee (\Psi \wedge \neg\Psi) \vdash \Phi \vee (\Psi \wedge \neg\Psi)}{\Phi \vee (\Psi \wedge \neg\Psi) \vdash \Phi}. \ \Box$$

PROOF OF THEOREM 5. Let X be a formula which is equivalent to Φ and is in cnf. There is such a formula by Theorem 3. Let $X_0, \ldots, X_k$ be all conjunctive terms of X for which there are no propositional variables P such that $P, \neg P \in D(X_i)$. There are such terms, since otherwise by Lemma 6 and Lemma 5 the formula X, and consequently Φ, would be provable.

Let $D(X_i) = \{X_i^0, \ldots, X_i^{k_i}\}$, where $X_i^r \neq X_i^s$ for $r \neq s$. By Corollary 1 an elementary disjunction X_i is equivalent to an elementary disjunction $X_i' = (\ldots(X_i^0 \vee X_i^1) \vee \ldots) \vee X_i^{k_i}$ in which each propositional variable occurs at most once. By Lemmas 6, 7 and the replacement theorem the formula X is equivalent to the formula $X' = (\ldots(X_0' \wedge X_1') \wedge \ldots) \wedge X_k'$. Let $P_0, \ldots, P_n$ be all atomic subformulas of the formula X'. Unless some X_j' contains some P_i as a subformula, by virtue of

$$X_j' \equiv X_j' \vee (P_i \wedge \neg P_i) \equiv (X_j' \vee P_i) \wedge (X_j' \vee \neg P_i)$$

the formula

$$X'' = (X')^{X_j'}_{(X_j' \vee P_i) \wedge (X_j' \vee \neg P_i)}$$

is equivalent to X, is in cnf, any propositional variable has at most one occurrence in any of its conjunctive terms and the number of its conjunctive terms containing no P_i is smaller than in X'. On carrying out a finite number of such transformations we can obtain a formula X^* equivalent to Φ and satisfying (1) and (2) of the definition of a formula in principal cnf. We choose the maximal set $\{\Psi_0, \ldots, \Psi_k\}$ of mutually nonequivalent conjunctive terms of X^*. Corollary 1 yields $D(\Psi_i \neq D(\Psi_j)$ for $i \neq j$. From the replacement theorem and Corollary 2 it follows that X^* is equivalent to the formula $\Psi = (\ldots(\Psi_0 \wedge \Psi_1) \wedge \ldots) \wedge \Psi_k$ and hence Ψ satisfies the requirements of the theorem. □

The proof of the next theorem is similar and we leave it to the reader as an exercise.

THEOREM 5′. *If a formula $\neg\Phi$ of PC is not PC-provable, then there is a formula Ψ which is equivalent to Φ and is in principal dnf.* □

Exercises

1. Prove statements (b) to (f) of Lemma 1 and statements (a), (a′), (b), (b′), (c′) of Lemma 4.

2. Prove Proposition 2, Theorem 4 and Theorem 5′.

3. Show that in Theorems 4 and 5 it is possible to require that Φ and Ψ should contain the same variables.

4. Show that the sequent $\Gamma, \Phi \vdash \Psi$ is PC-provable if and only if for any $X \in D(\Phi)$ the sequent $\Gamma, X \vdash \Psi$ is PC-provable.

6. SEMANTICS OF THE PROPOSITIONAL CALCULUS

A calculus is said to be *consistent* if not all formulas of that calculus are provable in it.

Let X be some set and let f_X be some mapping of elementary formulas of PC into the set $P(X)$ of all subsets of X. Such F_X will be called an *interpretation of PC in X*. We extend f_x to a mapping of the formulas of PC into $P(X)$ (we denote it also by f_X) by induction:

(1) $f_X(\Phi \wedge \Psi) = f_X(\Phi) \cap f_X(\Psi)$,

(2) $f_X(\Phi \vee \Psi) = f_X(\Phi) \cup f_X(\Psi)$,

(3) $f_X(\neg \Phi) = X \setminus f_X(\Phi)$,

(4) $f_X(\Phi \rightarrow \Psi) = f_X(\neg \Phi) \cup f_X(\Psi)$.

To each sequent S of PC we assign a statement $f_X(S)$ about the subsets of X in the following way:

(a) $f_X(\Phi_0, \ldots, \Phi_n \vdash \Phi) \Leftrightarrow$

$$\Leftrightarrow (f_X(\Phi_0), \ldots, f_X(\Phi_n) \rightarrow f_X(\Phi));$$

(b) $f_X(\vdash \Phi) \Leftrightarrow f_X(\Phi) = X$;

(c) $f_X(\Phi_0, \ldots, \Phi_n \vdash) \Leftrightarrow (f_X(\Phi_0), \ldots, f_X(\Phi_n) \rightarrow)$;

(d) $f_X(\vdash) \Leftrightarrow X \rightarrow$.

We recall (Section 1) the definition of the relation $\rightarrow$ on sets:

$$X_0, \ldots, X_n \rightarrow Y \Leftrightarrow \left(\bigcap_{i \leqslant n} X_i \subseteq Y\right);$$

$$(X_0, \ldots, X_n \rightarrow) \Leftrightarrow \left(\bigcap_{i \leqslant n} X_i = \varnothing\right).$$

THEOREM 6. *For any interpretation f_X of PC in X and any PC-provable sequent S the statement $f_X(S)$ is true.*

PROOF. Let D be a derivation tree in PC of the sequent S. It is obvious that if S' is an axiom, then $f_X(S')$ is true. Therefore it suffices to prove that if f_X of the sequents above the line in D is true, then f_X of the sequents beneath the same line is also true. For example, let

$$\frac{\Phi_0, \ldots, \Phi_n, \Psi_0 \vdash \mathrm{X};\ \Phi_0, \ldots, \Phi_n, \Psi_1 \vdash \mathrm{X};\ \Phi_0, \ldots, \Phi_n \vdash \Psi_0 \vee \Psi_1}{\Phi_0, \ldots, \Phi_n \vdash \mathrm{X}}$$

be a passage in the tree D and suppose that $f_X(\Phi_0, \ldots, \Phi_n, \Psi_0 \vdash \mathrm{X})$, $f_X(\Phi_0, \ldots, \Phi_n, \Psi_1 \vdash \mathrm{X})$, $f_X(\Phi_0, \ldots, \Phi_n \vdash \Psi_0 \vee \Psi_1)$ hold. Let $x \in \bigcap\limits_{i \leqslant n} f_X(\Phi_i)$. Since $\bigcap\limits_{i \leqslant n} f_X(\Phi_i) \subseteq f_X(\Psi_0) \cup f_X(\Psi_1)$, we have $x \in f_X(\Psi_j)$ for some $j \leqslant 1$. Since $\bigcap\limits_{i \leqslant n} f_X(\Phi_i) \cap f_X(\Psi_j) \subseteq f_X(\mathrm{X})$, we have $x \in f_X(\mathrm{X})$. Consequently, $f_X(\Phi_0, \ldots, \Phi_n \vdash \mathrm{X})$ holds.

Verification for the other passages of D is also simple and is left to the reader. □

COROLLARY 1. *PC is consistent.*

PROOF. Let X be a nonempty set and let f_X be some interpretation of PC in X. By the definition of an interpretation $f_X(Q_0 \wedge \neg Q_0) = f_X(Q_0) \cap (X \setminus f_X(Q_0)) = \varnothing$. It is obvious that the statement $f_X(\vdash Q_0 \wedge \neg Q_0)$ is false. By Theorem 6 the sequent $\vdash Q_0 \wedge \neg Q_0$ is not provable. Consequently, the formula $Q_0 \wedge \neg Q_0$ is not PC-provable. □

We have considered an interpretation of PC in which propositional variables were interpreted as subsets of some set X and logical connectives were interpreted as operations on those subsets. This made it possible to prove the consistency of PC. Also of interest is the parallelism itself of set-theoretic operations and logical connectives *.

Of course, the notion of interpretation exceeds the limits of the calculus itself. It relates to the so-called *semantics of the calculus*, in contrast to the notions of formula, rules of inference, proof, which relate to the *syntax of the calculus*.

We now consider another interpretation of PC which is very closely related to this interpretation and will be called the *principal interpretation of PC*. On the set $\{0, 1\}$ we define the operations $\wedge$, $\vee$, $\rightarrow$, $\neg$ by means of the following table:

---

* A useful generalization of this interpretation is given in Exercise 2 of Sec. 11.

x	y	$x \wedge y$	$x \vee y$	$x \rightarrow y$	$\neg x$
0	0	0	0	1	1
0	1	0	1	1	1
1	0	0	1	0	0
1	1	1	1	1	0

(1)

This table corresponds to rules (1) to (4) of the definition of an interpretation $f_{\{\varnothing\}}$ when $0 = \varnothing$, $1 = \{\varnothing\}$. Sometimes instead of 0, 1 the words "false" and "true" are used. Then the table will indicate rules of assigning truth values to the connectives $\wedge$, $\vee$, $\rightarrow$, $\neg$, which agree rather well with the use of the corresponding connectives in the English language.

Fix propositional variables $P_0, \ldots, P_k$. Given a mapping f of the set of elementary formulas $\{P_0, \ldots, P_k\}$ in $\{0, 1\}$, by table (1) f is uniquely extended to the set of formulas of PC whose propositional variables are among $P_0, \ldots, P_k$. If, besides, $f(\Phi) = 1$ ($f(\Phi) = 0$), then we shall say that on the set $\langle f(P_0), \ldots, f(P_k)\rangle$ *the truth value of the formula* Φ is 1 (0) or simply that Φ *is true* (*false*) *on this set*.

Thus, for any formula Φ with propositional variables among $P_0, \ldots, P_k$ we have a $(k + 1)$-place function on the set $\{0, 1\}$ which assigns to given truth values of the variables $P_0, \ldots, P_k$ the truth value of the formula Φ. This function will be called the *truth function of the formula* Φ (and denoted by $T_\Phi(P_0, \ldots, P_k)$). A formula Φ with variables among P_i, $i \leqslant k$, is said to be *identically true* (*identically false*) if $T_\Phi(P_0, \ldots, P_k)$ takes on the value of truth (falsehood) on all sets of values of the variables $P_0, \ldots, P_k$. It is clear that this concept does not depend on the choice of $P_0, \ldots$ $\ldots, P_k$. A sequent $\Gamma \vdash \Phi$ is said to be *true on the set* $\langle t_0, \ldots, t_k\rangle$ of truth values of the variables $P_0, \ldots, P_k$ which contain all the variables of the sequent $\Gamma \vdash \Phi$ if on the set $\langle t_0, \ldots, t_k\rangle$ either one of the formulas of Γ is false or Φ is true. The sequent $\Gamma \vdash$ is said to be *true on the set* $\langle t_0, \ldots, t_k\rangle$ of truth values of the variables $P_0, \ldots, P_k$ among which there are all the variables of the elements of Γ if one of the formulas of Γ is false on $\langle t_0, \ldots, t_k\rangle$. The sequent $\vdash$ is false on any set by definition and the truth of the sequent $\vdash \Phi$ coincides with that of Φ.

A sequent S is said to be *identically true* if it is true on any set $\langle t_0, \ldots, t_k \rangle$ of truth values of the variables $P_0, \ldots, P_k$ which contain all the variables occurring in S. It is obvious that these concepts are also independent of the choice of $P_0, \ldots, P_k$.

THEOREM 7. *If a sequent S of PC is PC-provable, then S is identically true.*

PROOF. Let D be a tree form proof in PC of the sequent S. We proceed by induction on the height of the proof D. If S is an axiom, then the statement of the theorem is trivial. To complete the proof it is necessary to verify that Rules 1 to 12 remain identically true. For example, let

$$\frac{\Gamma \vdash \Phi;\ \vdash \Phi \rightarrow \Psi}{\Gamma \vdash \Psi}$$

be an application of Rule 8. If on some set of truth values of the propositional variables all the formulas of Γ are true, then by the induction hypothesis Φ and $\Phi \rightarrow \Psi$ are true on that set. Hence by the definition of the operation $\rightarrow$ the formula Ψ is also true.

The verification of the other rules is also simple and we leave it to the reader.

Theorem 7 yields another proof of Corollary 1. Indeed, it is clear that $Q_0 \wedge \neg Q_0$ is an identically false formula. By virtue of Theorem 7 therefore the sequent $\vdash Q_0 \wedge \neg Q_0$ is not PC-provable.

COROLLARY 2. *If $\Phi \equiv \Psi$ and the propositional variables of Φ and Ψ are contained among $P_0, \ldots, P_k$, then $T_\Phi(P_0, \ldots, P_k) = T_\Psi(P_0, \ldots, P_k)$.*

PROOF. Suppose that on a set $\bar{t}$ we have $T_\Phi(\bar{t}) = 1$. Under the hypothesis $\Phi \vdash \Psi$ is provable. By Theorem 7 we get $T_\Psi(\bar{t}) = 1$. Similarly $T_\Psi(\bar{t}) = 1$ yields $T_\Phi(\bar{t}) = 1$. □

We introduce the notation $P^0 = P$, $P^1 = \neg P$. Let $\bar{t} = \langle t_0, \ldots, t_n \rangle$ be a set of zeros and unities.

LEMMA 1. *An elementary disjunction Φ of the form $P_0^{t_0} \vee \ldots \vee P_n^{t_n}$ takes on the value "0" on a unique set $\bar{t} = \langle t_0, \ldots, t_n \rangle$ of truth values of the variables $P_0, \ldots, P_n$.*

PROOF. The formula Φ is constructed from formulas $P_i^{t_i}$ by means of the operation $\vee$. It follows from the truth table that if one of the formulas $P_i^{t_i}$ assumed a value of 1, then Φ would also assume a value of 1. Hence P_i must assume a value t_i. □

THEOREM 8 (Functional Completeness of PC). *Let f be a function defined on the sets $\langle t_0, \ldots, t_n \rangle$ of zeros and unities and taking on zero or unit as its value. Then there is a formula of PC such that its variables are contained among $Q_0, \ldots, Q_n$ and $T_\Phi(Q_0, \ldots, Q_n) = f$.*

PROOF. If f is identically one, then we can take the formula $Q_0 \vee \neg Q_0$ as Φ.

We denote a suit $\langle t_1, \ldots, t_n \rangle$ of elements of the set $\{0, 1\}$ by $\bar{t}$ and by $f(\bar{t})$ the value of $f(t_1, \ldots, t_n)$. Let the set $X = \{\bar{t} \mid f(\bar{t}) = = 0\}$ be nonempty. Take as Φ a formula of the form $\bigwedge\limits_{\bar{t} \in X} (P_1^{t_1} \vee \ldots \vee P_n^{t_n})$. We prove that $T_\Phi(\bar{t}) = 0$ is equivalent to $\bar{t} \in X$. Let $T_\Phi(\bar{t}) = 0$. Since Φ is constructed from conjunctive terms using the operation $\wedge$, there is a conjunctive term Ψ which is false on the set $\bar{t}$. Ψ has the form $P_1^{t_1'} \vee \ldots \vee P_n^{t_n'}$, where $\bar{t}\,' \in X$. By virtue of the preceding lemma $\bar{t}\,' = \bar{t}$ and hence $\bar{t} \in X$. Now let $\bar{t} \in X$. By Lemma 1 a conjunctive term Ψ of the form $P_1^{t_1} \vee \ldots \vee P_n^{t_n}$ is false on $\bar{t}$. Again using the fact that Φ is constructed from conjunctive terms (with Ψ among them) with the aid of the operation $\wedge$ we conclude that $T_\Phi(\bar{t}) = 0$. □

Exercises

1. Suppose that your computational capabilities consist only in the following: given a pair of numbers $t_1, t_2 \in \{0, 1\}$ you can compute the maximum $\max(t_1, t_2)$ of those numbers and given $t \in \{0, 1\}$ you can name $\bar{t} \in \{0, 1\}$ which is not equal to t. Show that in this case you are capable of computing any function f assigning to suites $\langle t_0, \ldots, t_n \rangle$ of zeros and unities, zero or unity. Namely, for any such function f there is a sequence $s_0, \ldots, s_k$ such that for any $i \leqslant k$ s_i is either a pair $\langle j, m \rangle$ of numbers smaller than i or a single number smaller than i. Moreover, if by the given suite $\langle t_0, \ldots, t_n \rangle$ of zeros and unities you write a sequence $q_0, \ldots, q_k$ of zeros and unities according to the following rule:

(a) if $i \leqslant n$, then $q_i = t_i$;

(b) if $n < i \leqslant k$ and $s_i = \langle j, m \rangle$, then $q_i = \max(q_j, q_m)$;

(c) if $n < i \leqslant k$ and $s_i < i$, then $q_i = \tilde{q}_{s_i}$, then q_k will be the value of f on $\langle t_0, \ldots, t_n \rangle$. (*Hint*. Use Theorem 8. Corollary 2 and the equivalence $\Phi \wedge \psi \equiv \equiv \neg(\neg\Phi \vee \neg\Psi)$.)

2. Show that if formulas $\Phi \equiv \Psi$ are in principal cnf (principal dnf) and contain the same variables, then $\{D(X) \mid X \in K(\Phi)\} = \{D(X) \mid X \in K(\Psi)\}$ ($\{K(X) \mid X \in D(\Phi)\} = \{K(X) \mid X \in D(\Psi)\}$).

7. CHARACTERIZATION OF PROVABLE FORMULAS

THEOREM 9. *Let Φ be a formula of PC. The following three conditions are equivalent:*

(1) *Φ is PC-provable.*

(2) *For any $\Phi' \equiv \Phi$ which is in cnf and any of its conjunctive terms Ψ there is an atomic formula P such that $P, \neg P \in D(\Psi)$.*

(3) *There is $\Phi' \equiv \Phi$ which is in cnf and is such that for any of its conjunctive terms Ψ there is an atomic P such that $P, \neg P \in D(\Psi)$.*

PROOF. (2) ⇒ (3) is trivial, (3) ⇒ (1) follows from Lemmas 5.5, 5.6 and 4.2(a).

We prove (1) ⇒ (2). Let Φ be provable. Then any conjunctive term Ψ of the formula Φ' is provable by virtue of Lemma 5.5. Let $D(\Psi)$ contain no atomic formula P together with its negation $\neg P$. Consider two sets of atomic formulas, $X = \{P \mid P \in D(\Psi)\}$ and $Y = \{P \mid \neg P \in D(\Psi)\}$. Under the hypothesis $X \cap Y = \varnothing$. Let Ψ_1 be obtained from Ψ by replacing all subformulas $P \in X$ by Q_0 and all $P \in Y$ by $\neg Q_0$. By the substitution theorem Ψ_1 is provable. Let Ψ_2 be obtained from Ψ_1 be replacing $\neg\neg Q_0$ by Q_0. By Lemma 5.1(b) and the replacement theorem $\Psi_2 \equiv \Psi_1$. Hence Ψ_2 is provable. It is obvious that $D(\Psi_2) = \{Q_0\}$. By Corollary 5.1 $Q_0 \equiv \Psi_2$. Hence Q_0 is provable. From the substitution theorem we conclude that any formula of X is provable. This is impossible by virtue of the consistency of PC. ☐

Theorem 9 gives a characterization of PC-provable formulas based on the structure of formulas which are equivalent to them and are in cnf. Such a characterization will be called *deductive*. Now we obtain a *semantic characterization* of PC-provable formulas based on the notion of truth.

LEMMA 1. *The sequent* $\Gamma, \Phi \vdash \Psi$ *is provable if and only if so is the sequent* $\Gamma \vdash \Phi \to \Psi$.

PROOF follows immediately from Rules 7 and 8. □

LEMMA 2. *The sequent* $\Gamma \vdash$ *is provable if and only if so is the sequent* $\Gamma \vdash Q_0 \wedge \neg Q_0$.

PROOF follows from Proposition 3.2(c) and (g). □

THEOREM 10 (Completeness of PC). (a) *For a formula* Φ *of PC to be PC-provable it is necessary and sufficient that* Φ *is identically true.*

(b) *For a sequent S of PC to be PC-provable it is necessary and sufficient that S is identically true.*

PROOF. Necessity is asserted by Theorem 7. Statement (b) follows from (a), since by virtue of Lemmas 1, 2 and the definition of the identical truth of sequents and formulas the provability and identical truth of the sequents $\Phi_1, \ldots, \Phi_n \vdash \Psi$ and $\Phi_1, \ldots, \Phi_n \vdash$ are equivalent to the provability and identical truth of the formulas $\Phi_1 \to (\Phi_2 \to \ldots \to (\Phi_n \to \Psi)\ldots)$ and $\Phi_1 \to (\Phi_2 \to \ldots \to (\Phi_n \to Q_0 \wedge \neg Q_0)\ldots)$ respectively.

Let Φ be an identically true formula and let $\Phi' \equiv \Phi$ be in cnf. Suppose that Φ is not provable. Then Φ' is not provable either. By Lemmas 5.5 and 5.6 there is a conjunctive term Ψ of the formula Φ' such that $D(\Psi)$ contains no atomic formula P together with its negation $\neg P$. Let $X = \{P \mid P \in D(\Psi)\}$ and $Y = \{P \mid \neg P \in D(\Psi)\}$. Then $X \cap Y = \varnothing$. If the variables of X take on a value 0 and the variables of Y take on a value 1, then by Lemma 6.1 Ψ takes on a value 0. Since Φ' is constructed from conjunctive terms (Ψ among them) using one connective $\wedge$, Φ' takes on a value 0 when the variables of X take on a value 0 and those of Y take on a value 1. Hence Φ' is not an identically true formula. By Corollary 6.2 Φ is not an identically true formula either. A contradiction. □

If a calculus is given and the concept of truth (semantics) of the formulas of that calculus is defined, then the calculus is said to be *consistent with respect to the semantics* if only true formulas are provable in the calculus. If all true formulas are provable, then the calculus is said *to be complete for the semantics.* Of great importance besides the problem of consistency and completeness is the *problem of solvability of calculus.* A calculus is said to be *solvable* if there is an effective procedure (algorithm) allowing one to determine for any formula Φ in a finite number of steps whether or not Φ is provable. If there is no such procedure, then the calculus is said to be unsolvable or *undecidable*.

If the truth of the formulas of PC is defined as identical truth, then the previous theorem shows that PC is complete and consistent for this semantics. It is obvious that it is possible to find out in a finite number of steps whether or not a given formula Φ of PC is identically true. Since the identical truth and the provability of Φ are equivalent, PC is solvable.

When a calculus is given using axiom schemata and rules of inference the question naturally arises as to whether the axiom schemata and rules of inference are independent. An *axiom schema* is said to be *independent* in a calculus if at least one of its special instances is not provable in the calculus without that schema. A *rule of inference* is said to be *independent* in a calculus if it is not admissible in the calculus without that rule. A *calculus* is said to be *independent* if all of its axiom schematas and rules of inference are independent.

When constructing a calculus one often aims at obtaining an independent calculus. (Of no small importance here are aesthetic considerations.) In the remainder of this section we use PC as an example to present an important method of proving the independence of calculi *.

PROPOSITION 1. *PC is independent.*

PROOF. Since there is only one axiom schema in PC, this schema is independent. To prove the independence of the rules of inference it is sufficient to find for every rule α a characteristic property Δ which is peculiar to all sequents provable using rules distinct from α and which some of the PC-provable sequents fail to possess. We restrict ourselves only to formulations of characteristic properties for Rules 1 to 12, leaving the necessary verification of the reader.

A characteristic property of Rules 1 to 8 is the identical truth (Sec. 6) of sequents when a new definition is given to each rule of one of the logical operations $\wedge$, $\vee$, $\rightarrow$, $\neg$ on the set $\{0, 1\}$. The other operations are defined using the table of Sec. 6. Here are the new definitions of logical operations corresponding to Rules 1 to 8.

---

* See also Exercise 8.1.

Rule 1. The conjunction is defined to be an identically false function.

Rule 2. The value of the conjunction $x \wedge y$ is equal to the value of the second term, y.

Rule 3. The value of the conjunction $x \wedge y$ is equal to the value of the first term, x.

Rule 4. The value of the disjunction $x \vee y$ is equal to that of the second term, y.

Rule 5. The value of the disjunction $x \vee y$ is equal to that of the first term, x.

Rule 6. The disjunction is defined to be an identically true function.

Rule 7. The implication is defined to be an identically false function.

Rule 8. The implication is defined to be an identically true function.

Consider a set $A = \{0, 1, 2,\}$. A conjunction on the set A is defined to be a minimum of two numbers and a disjunction is defined to be a maximum of two numbers. Negation is defined as follows: $\neg(2) = 0$, $\neg(1) = 0$, $\neg(0) = 2$. Implication is defined thus:

$$m \rightarrow n = \begin{cases} 2, & m \leqslant n; \\ n, & m > n. \end{cases}$$

Rule 9. A characteristic property for sequents $\Gamma \vdash \Phi$ $(\Gamma \vdash)$ is the following: for the values from the set A of the propositional variables the minimum of the values of the formulas of Γ is less than or equal to the value of the formula Φ (is equal to zero, respectively). The minimum of an empty set of values is assumed equal to two.

Rule 10. A characteristic property of sequents for this rule is the presence of a formula on the right-hand side.

Rule 11. A characteristic property of sequents $\Gamma \vdash \Phi$ $(\Gamma \vdash)$ is that: if $\Gamma = \langle \Phi_0, \ldots, \Phi_n \rangle \neq \varnothing$, then the sequent $\Phi_0 \vdash \Phi$ $(\Phi_0 \vdash)$ is PC-provable.

Rule 12. A characteristic property of the sequents $\Gamma \vdash \Phi$, $\Gamma \vdash$ is that Γ has one element or is empty. □

Exercises

1. Let a formula Φ of PC be in dnf. For Φ to be PC-provable, it is necessary and sufficient that for any sets X and Y of propositional variables containing no elements in common there is a formula $\Psi \in D(\Phi)$ and sets X_1 and Y_1 of propositional variables such that $(X \cup X_1) \cap (Y \cup Y_1) = \varnothing$ and $K(\Psi) \subseteq \{P \mid P \in (X \cup X_1) \cup \{\neg P \mid P \in (Y \cup Y_1)\}$. (*Hint.* Use the PC completeness theorem.)

2. Make the necessary verification of the characteristic properties in the proof of Proposition 1.

8. HILBERTIAN PROPOSITIONAL CALCULUS

In this section we shall treat an alternative, the so-called Hilbertian, axiomatization of propositional calculus, PC_1.

DEFINITION. The notion of formula in PC_1 is the same as in PC; there are no sequents in PC_1. The axioms of PC_1 are obtained from the following ten schematas by substituting concrete formulas of PC_1 for the variables Φ, Ψ, X.

1. $\Phi \to (\Psi \to \Phi)$,
2. $(\Phi \to \Psi) \to ((\Phi \to (\Psi \to \mathrm{X})) \to (\Phi \to \mathrm{X}))$,
3. $(\Phi \wedge \Psi) \to \Phi$,
4. $(\Phi \wedge \Psi) \to \Psi$,
5. $(\Phi \to \Psi) \to ((\Phi \to \mathrm{X}) \to (\Phi \to (\Psi \wedge \mathrm{X})))$,
6. $\Phi \to (\Phi \vee \Psi)$,
7. $\Phi \to (\Psi \vee \Phi)$,
8. $(\Phi \to \mathrm{X}) \to ((\Psi \to \mathrm{X}) \to ((\Phi \vee \Psi) \to \mathrm{X}))$,
9. $(\Phi \to \Psi) \to ((\Phi \to \neg\Psi) \to \neg\Phi)$,
10. $\neg\neg\Phi \to \Phi$.

There is only one rule of inference in PC_1:

$$\frac{\Phi, \Phi \to \Psi}{\Psi}.$$

DEFINITION. A *proof in* PC_1 of a formula Φ_n is a sequence of formulas $\Phi_0, \ldots, \Phi_n$ of PC_1 such that each Φ_i, $i \leqslant n$ is either an axiom or is obtained from some Φ_j, Φ_k, $j, k < i$, by the rule of inference. If there is a proof in PC_1 of a formula Φ, then Φ is said to be PC_1*-provable* and this is designated $\rhd \Phi$. A *derivation in* PC_1

of a formula Φ_n *from a set H of formulas of* PC_1 is a sequence $\Phi_0, \ldots, \Phi_n$ of formulas of PC_1 such that each Φ_i, $i \leqslant n$, is either an axiom or is in H, or is obtained from some Φ_j, Φ_k, $j, k < i$, by the rule of inference. If there is a derivation of a formula Φ from H, then Φ is said to be PC_1*-derivable from H* and we write $H \rhd \Phi$, with H called a *set of hypotheses*.

It is obvious that the PC_1-provability of Φ is equivalent to the PC_1-derivability of Φ from an empty set of hypotheses. Note that H need not be a finite set of hypotheses, but if $H \rhd \Phi$, then by virtue of the finiteness of the derivation of Φ from H there is a finite set $H_1 \subseteq H$ such that $H_1 \rhd \Phi$. It is also obvious that if $H \subseteq H'$ and $H \rhd \Phi$, then $H' \rhd \Phi$.

The main purpose of this section is to prove the following theorem which shows in a certain sense the equivalence of PC and PC_1.

THEOREM 11. (a) *A sequent* $\Psi_1, \ldots, \Psi_n \vdash \Phi$ *is PC-provable if and only if* Φ *is* PC_1*-derivable from* $\{\Psi_1, \ldots, \Psi_n\}$. *In particular, the sets of PC- and* PC_1*-provable formulas coincide.*

(b) *A sequent* $\Psi_1, \ldots, \Psi_n \vdash$ *is PC-provable if and only if the formula* $Q_0 \wedge \neg Q_0$ *is* PC_1*-derivable from* $\{\Psi_1, \ldots, \Psi_n\}$.

Before proving Theorem 11 we develop some theory of PC_1-derivability.

EXAMPLE 1. Let Φ be a formula of PC_1. A sequence of the following five formulas will be a proof of the formula $\Phi \to \Phi$ in PC_1:

(1) $\Phi \to (\Phi \to \Phi)$ is an axiom,

(2) $\Phi \to ((\Phi \to \Phi) \to \Phi)$ is an axiom,

(3) $(\Phi \to (\Phi \to \Phi)) \to ((\Phi \to ((\Phi \to \Phi) \to \Phi)) \to (\Phi \to \Phi))$ is an axiom,

(4) $(\Phi \to ((\Phi \to \Phi) \to \Phi)) \to (\Phi \to \Phi)$ by the rule of inference for (1) and (3).

(5) $\Phi \to \Phi$ by the rule of inference for (2) and (4).

A rule of inference

$$\frac{\Phi_0, \ldots, \Phi_k}{\Psi}$$

is said to be PC_1*-admissible* if its addition to PC_1 does not enlarge the family of formulas derivable from H for any set of hypotheses H.

A *quasi-derivation in* PC_1 *of a formula* Φ_n *from a set of hypotheses* H is a sequence of formulas $\Phi_0, \ldots, \Phi_n$ such that each Φ_i, $i \leqslant n$, is either PC_1-derivable from H or is obtained from some preceding formulas by a PC_1-admissible rule of inference. It is obvious that if there is a quasi-derivation in PC_1 of a formula Φ from the set H, then Φ is PC_1-derivable from H.

THEOREM 12 (Deduction). *If* $H \cup \{\Phi\} \rhd \Psi$, then $H \rhd \Phi \to \Psi$.

PROOF. By induction on the minimal n for which there is a derivation $\Psi_0, \ldots, \Psi_n$ of a formula Ψ from $H \cup \{\Phi\}$. If $n = 0$, then either (1) $\Psi = \Phi$ or (2) Ψ is an axiom or occurs in H. In the former case, by virtue of Example 1 the formula $\Phi \to \Psi$ is derivable from H. In the latter case the sequence

$$\Psi,\ \Psi \to (\Phi \to \Psi),\ \Phi \to \Psi$$

is a derivation in PC_1 from H. Let $n > 0$. From the minimality of n we conclude that Ψ is obtained from Ψ_i and that $\Psi_j = (\Psi_i \to \Psi)$ for $i, j < n$ by the rule of inference. Then by the induction hypothesis the sequence

$$\Phi \to \Psi_i,\ \Phi \to (\Psi_i \to \Psi),$$
$$(\Phi \to \Psi_i) \to ((\Phi \to (\Psi_i \to \Psi)) \to (\Phi \to \Psi)),$$
$$(\Phi \to (\Psi_i \to \Psi)) \to (\Phi \to \Psi),\ \Phi \to \Psi$$

is a quasi-derivation of $\Phi \to \Psi$ from H. □

For many formulas of PC_1 the deduction theorem facilitates substantially the establishment of their PC_1 provability. Thus, in the following example but for the deduction theorem it would be necessary to give a much more lengthy proof.

EXAMPLE 2. Let Φ and Ψ be formulas of PC_1. We show that the formula $\Phi \to (\Psi \to (\Phi \wedge \Psi))$ is PC_1-provable. By the deduction theorem it suffices to show that $\{\Phi, \Psi\} \rhd \Phi \wedge \Psi$. The following sequence is the required derivation:

(1) $\Phi \to (\Phi \to \Phi)$ is an axiom,
(2) $\Psi \to (\Phi \to \Psi)$ is an axiom,
(3) $(\Phi \to \Phi) \to ((\Phi \to \Psi) \to (\Phi \to \Phi \wedge \Psi)))$ is an axiom,
(4) Φ is a hypothesis,
(5) $\Phi \to \Phi$ by the rule for (1) and (4),
(6) Ψ is a hypothesis,

(7) $\Phi \to \Psi$ by the rule for (2) and (6),
(8) $(\Phi \to \Psi) \to (\Phi \to (\Phi \wedge \Psi))$ by the rule for (3) and (5),
(9) $\Phi \to (\Phi \wedge \Psi)$ by the rule for (7) and (8),
(10) $\Phi \wedge \Psi$ by the rule for (4) and (9).

Before proving Theorem 11 we establish one more technical fact.

COROLLARY 1. $\{\Phi_0, \ldots, \Phi_n\} \rhd \Phi$ *is equivalent to* $\rhd \Phi_0 \to (\Phi_1 \to \ldots (\Phi_n \to \Phi)\ldots)$ *which is in turn equivalent to* $\rhd (\Phi_0 \wedge (\Phi_1 \wedge \ldots (\Phi_{n-1} \wedge \Phi_n)\ldots)) \to \Phi$.

PROOF. In one direction we apply the deduction theorem $n + 1$ times. Now let $\rhd \Phi_0 \to (\Phi_1 \to \ldots (\Phi_n \to \Phi)\ldots)$. Then $\{\Phi_0, \ldots, \Phi_n\} \rhd \Phi_0 \to (\Phi_1 \to \ldots (\Phi_n \to \Phi)\ldots)$ and applying the rule of inference several times we get $\{\Phi_0, \ldots, \Phi_n\} \rhd \Phi$. Using several times Example 2 and the rule of inference we get $\{\Phi_0, \ldots, \Phi_n\} \rhd \Phi_0 \wedge (\Phi_1 \wedge \ldots (\Phi_{n-1} \wedge \Phi_n)\ldots)$ and applying several times Axioms 3, 4, and the rule of inference we get $\{\Phi_0 \wedge (\Phi_1 \wedge \ldots (\Phi_{n-1} \wedge \Phi_n)\ldots)\} \rhd \Phi_i$ for any $i \leqslant n$. Hence $\{\Phi_0, \ldots, \Phi_n\} \rhd \Phi$ is equivalent to the derivability of $\{\Phi_0 \wedge (\Phi_1 \wedge \ldots (\Phi_{n-1} \wedge \Phi_n)\ldots)\} \rhd \Phi$, which has already been shown above to be equivalent to $\rhd (\Phi_0 \wedge (\Phi_1 \wedge \ldots (\Phi_{n-1} \wedge \Phi_n)\ldots) \to \Phi$. □

PROOF OF THEOREM 11. By virtue of Corollary 1 and Lemmas 7.1, 7.2 it suffices to show that the PC provability of Φ is equivalent to the PC_1 provability of Φ. It is easy to verify that all the axioms of PC_1 are identically true and that the rule of inference of PC_1 remains identically true. By the PC completeness theorem therefore $\rhd \Phi$ implies the PC provability of Φ.

We shall say that *a rule of inference of PC remains derivable in* PC_1 if after replacing in it the sequents $\Psi_1, \ldots, \Psi_n \vdash \Phi$ and $\Psi_1, \ldots, \Psi_n \vdash$ by $\{\Psi_1, \ldots, \Psi_n\} \rhd \Phi$ and $\{\Psi_1, \ldots, \Psi_n\} \rhd Q_0 \wedge \neg Q_0$ respectively, the truth of the statements above the line will imply the truth of the statement below the line. It is clear that to prove that the PC provability of Φ implies $\rhd \Phi$ it suffices to show that Rules 1 to 12 remain derivable in PC_1. That Rules 1 to 5 remain derivable is easy to show using Example 2 and Axioms 3 to 7. Let $\{\Psi_1, \ldots, \Psi_k, \Phi\} \rhd \Psi$; $\{\Psi_1, \ldots, \Psi_k, X\} \rhd \Psi$; $(\Psi_1, \ldots, \Psi_k\} \rhd \Phi \vee X$.

By the deduction theorem

$$\{\Psi_1, \ldots, \Psi_k\} \rhd \Phi \to \Psi \quad \text{and} \quad \{\Psi_1, \ldots, \Psi_k\} \rhd X \to \Psi.$$

Applying the rule of inference of PC_1 to Axiom 8 three times we get $\{\Psi_1, \ldots, \Psi_k\} \rhd \Psi$. Hence Rule 6 remains derivable. Rule 7 corresponds to the deduction theorem, Rule 8 corresponds to the rule of inference of PC_1. We prove that Rule 9 remains derivable. Let $\{\Psi_1, \ldots, \Psi_k, \neg\Phi\} \rhd Q_0 \wedge \neg Q_0$. From Axioms 3 and 4 we get $\{\Psi_1, \ldots, \Psi_k, \neg\Phi\} \rhd Q_0$ and $\{\Psi_1, \ldots, \Psi_k, \neg\Phi\} \rhd$ $\rhd \neg Q_0$. By the deduction theorem we get

$$\{\Psi_1, \ldots, \Psi_k\} \rhd \neg\Phi \to Q_0 \text{ and } \{\Psi_1, \ldots, \Psi_k\} \rhd \neg\Phi \to \neg Q_0.$$

Then Axioms 9 and 10 yield $\{\Psi_1, \ldots, \Psi_k\} \rhd \Phi$. Consider Rule 10. Let $\{\Psi_1, \ldots, \Psi_k\} \rhd \Phi$ and $\{\Psi_1, \ldots, \Psi_k\} \rhd \neg\Phi$. From Axiom 1 we get

$$\{\Psi_1, \ldots, \Psi_k\} \rhd \neg(Q_0 \wedge \neg Q_0) \to \Phi$$

and

$$\{\Psi_1, \ldots, \Psi_k\} \rhd \neg(Q_0 \wedge \neg Q_0) \to \neg\Phi.$$

Axioms 9 and 10 then yield $\{\Psi_1, \ldots, \Psi_k\} \rhd Q_0 \wedge \neg Q_0$. That Rules 11 and 12 remain derivable follows immediately from the definition of derivation in PC_1. □

Exercise

1. Prove that PC_1 is independent. (*Hint*. Use the same method as for PC. To prove that Schemata 1 and 2 are independent the logical connectives are defined on the set $\{0, 1, 2\}$ and to prove that schemata 3 to 10 are independent the logical connectives are defined on the set $\{0, 1\}$. For Schema 1 the connectives are defined like this: $(n \wedge m) = \min(n, m)$, $n \vee m = \max(n, m)$, $\neg 0 = \neg 1 = 2$, $\neg 2 = 0$, $(n \to m) = 2$ if $n \leqslant m$ and $(n \to m) = 0$ if $n > m$. For Schema 2 we have: $(0 \wedge m) = (m \wedge 0) = 1$, $(0 \vee 0) = 1$, $\neg 2 = 1$, $(0 \to 0) = (2 \to 0) =$ $= (2 \to 1) = 1$, $(1 \to 0) = 2$ and the other values of the connectives are as for Schema 1. The characteristic property of formulas in proving the independence of Schemata 1 and 2 is that of being identically two.

9. CONSERVATIVE EXTENSION OF CALCULI

Given two languages $L_0 \subseteq L_1$ and two calculi, I_0 of L_0 and I_1 of L_1. I_1 is said to be a *conservative extension* of I_0 (designated $I_0 < I_1$) if an expression Φ of L_0 is I_0-provable if and only if Φ is

I_1-provable. It is obvious that the relation $<$ is reflexive, transitive and we have

PROPOSITION 1. *If $I_0 < I_1$ and I_0 is consistent, then I_1 is consistent.* $\square$

Let $\mathrm{PC}^{(\rightarrow)}$ be the calculus obtained from PC by removing from the alphabet the symbol $\rightarrow$ and dropping Rules 7 and 8.

PROPOSITION 2. $PC^{(\rightarrow)} < PC$.

PROOF. Let $\alpha\colon F \rightarrow F$ be the mapping defined in the proof of Lemma 5.2. We extend α to sequences of formulas and sequents:

$$\alpha(\langle \Phi_1, \ldots, \Phi_n \rangle) = \langle \alpha\Phi_1, \ldots, \alpha\Phi_n \rangle,$$
$$\alpha(\Gamma \vdash \Phi) = \alpha(\Gamma) \vdash \alpha(\Phi), \quad \alpha(\Gamma \vdash) = \alpha(\Gamma) \vdash .$$

Since $\alpha(\Phi) = \Phi$ for a formula Φ without implication, it suffices to show that if a sequent S is PC-provable, then the sequent $\alpha(S)$ is $\mathrm{PC}^{(\rightarrow)}$-provable. If D is a tree form proof of the sequent S in PC, then by induction on the height of D we shall construct a quasi-derivation D^* of the sequent $\alpha(S)$ in $\mathrm{PC}^{(\rightarrow)}$. If D is an axiom for PC, then it is obvious that $D^* = \alpha(D)$ is an axiom for $\mathrm{PC}^{(\rightarrow)}$. Let

$$D = \frac{D_1; \ldots; D_n}{S}.$$

If the last passage in D is effected by rules different from Rules 7 and 8, then obviously

$$D^* = \frac{D_1^*; \ldots; D_n^*}{\alpha(S)}$$

will be a quasi-derivation in $\mathrm{PC}^{(\rightarrow)}$ in which the last passage is effected by the same rule as in D. If

$$D = \frac{D_1; D_2}{\Gamma \vdash \Phi},$$

where D_1, D_2 are proofs in PC of sequents $\Gamma \vdash \Psi$, $\Gamma \vdash \Psi \rightarrow \Phi$ respectively, then as D^* we take the following tree:

$$\dfrac{\dfrac{D_1^* \qquad \dfrac{\neg\alpha(\Psi) \vdash \neg\alpha(\Psi); \quad \dfrac{\neg\alpha(\Phi), \alpha(\Phi), \neg\neg\alpha(\Psi) \vdash}{\neg\alpha(\Phi), \alpha(\Phi) \vdash \neg\neg\alpha(\Psi)}; D_2^*}{\alpha(\Gamma), \neg\alpha(\Phi) \vdash \neg\alpha(\Psi)}}{\alpha(\Gamma), \neg\,\alpha(\Phi) \vdash}}{\alpha(\Gamma) \vdash \alpha(\Phi)}$$

If

$$D = \frac{D_1}{\Gamma \vdash \Psi \to \Phi},$$

where D_1 is a proof in PC of the sequents $\Gamma, \Psi \vdash \Phi$, then as D^* we take the following tree:

$$\frac{\dfrac{D_1^*}{\alpha(\Gamma), \alpha(\Psi) \vdash \neg\alpha(\Psi) \vee \alpha(\Phi)}; \quad \neg\alpha(\Psi) \vdash \neg\alpha(\Psi) \vee \alpha(\Phi); \quad \vdash \alpha(\Psi) \vee \neg\alpha(\Psi)}{\alpha(\Gamma) \vdash \neg\alpha(\Psi) \vee \alpha(\Phi)}. \ \square$$

Let $PC^{(\to, \vee)}$ be the calculus obtained from PC by removing from the alphabet the symbols $\to$, $\vee$ and dropping Rules 4 to 8.

PROPOSITION 3. $PC^{(\to, \vee)} < PC$.

PROOF. We denote the set of formulas of PC without the symbol $\to$ by $F^{(\to)}$. We define a mapping β: $F^{(\to)} \to F^{(\to)}$ as follows:

(a) if Φ contains no sign $\vee$, then $\beta(\Phi) = \Phi$;

(b) if $\Phi = (\Psi \vee X)$, then $\beta(\Phi) = \neg(\neg\beta(\Psi) \wedge \neg\beta(X))$;

(c) if $\Phi = (\Psi \wedge X)$, $\Phi = \neg\Psi$, then $\beta(\Phi) = (\beta(\Psi) \wedge \beta(X))$, $\beta(\Phi) = \neg\beta(\Psi)$.

We extend β to sequences of formulas and sequents:

$$\beta(\langle \Phi_1, \ldots, \Phi_n \rangle) = \langle \beta\Phi_1, \ldots, \beta\Phi_n \rangle,$$

$$\beta(\Gamma \vdash \Phi) = \beta(\Gamma) \vdash \beta(\Phi), \quad \beta(\Gamma \vdash\ ) = \beta(\Gamma) \vdash .$$

By virtue of (a) of the definition of β and Proposition 2 it suffices to show that if the sequent S is $PC^{(\to)}$-provable, then $\beta(S)$ is $PC^{(\to, \vee)}$-provable.

For any tree form proof D of the sequent S in $PC^{(\to)}$ we shall construct by induction on height a quasi-derivation D^* of a sequent $\beta(S)$ in $PC^{(\to, \vee)}$. If D is an axiom of $PC^{(\to)}$, then it is obvious that $D^* = \beta(D)$ is an axiom of $PC^{(\to, \vee)}$. Let

$$D = \frac{D_0; \ldots; D_n}{S}.$$

If the last passage in D is effected by rules different from Rules 4 to 6 for PC, then it is obvious that

$$D^* = \frac{D_0^*; \ldots; D_n^*}{\beta(S)}$$

will be a quasi-derivation in $PC^{(\to, \vee)}$.

Let

$$D = \frac{D_1}{\Gamma \vdash \Phi \vee \Psi}$$

and let the last passage in D be effected by Rule 4 for PC. Then D_1^* will be a quasi-derivation of the sequent $\beta(\Gamma) \vdash \beta(\Phi)$ and we may take the following tree as D^*:

$$\cfrac{\cfrac{D_1^*;\ \beta(\Gamma),\ \neg\beta(\Phi) \wedge \neg\beta(\Psi) \vdash \neg\beta(\Phi)}{\beta(\Gamma),\ \neg\beta(\Phi) \wedge \neg\beta(\Psi) \vdash}}{\beta(\Gamma) \vdash \neg(\neg\beta(\Phi) \wedge \neg\beta(\Psi))}.$$

Similarly treated is the case where the last passage in D is an application of Rule 5.

Before treating the case where Rule 6 is applied we prove the $PC^{(\neg, \vee)}$ admissibility of the following rules:

$$\text{(a)}\ \frac{\Gamma, \Phi \vdash \Psi}{\Gamma, \neg\neg\Phi \vdash \Psi}; \qquad \text{(b)}\ \frac{\Gamma, \Phi \vdash}{\Gamma, \neg\neg\Phi \vdash};$$

$$\text{(c)}\ \frac{\Gamma, \Phi \vdash}{\Gamma \vdash \neg\Phi}; \qquad \text{(d)}\ \frac{\Gamma, \Phi \vdash \Psi}{\Gamma, \neg\Psi \vdash \neg\Phi}.$$

The $PC^{(\neg, \vee)}$ admissibility of rules (a) and (b) will be demonstrated simultaneously by induction on the height of the proof D in $PC^{(\neg, \vee)}$ of the sequents $\Gamma, \Phi \vdash \Psi$ ($\Gamma, \Phi \vdash$). If D is the axiom $X \vdash X$, then the quasi-derivation in $PC^{(\neg, \vee)}$ of the sequent $\neg\neg X \vdash X$ will be the following tree:

$$\cfrac{\cfrac{\neg X \vdash \neg X;\ \neg\neg X \vdash \neg\neg X}{\neg\neg X, \neg X \vdash}}{\neg\neg X \vdash X}.$$

If D is not an axiom, then the provability of the sequent $\Gamma, \neg\neg\Phi \vdash \Psi$ (the sequent $\Gamma, \neg\neg\Phi \vdash$) is immediate from the induction hypothesis. Let a sequent $\Gamma, \Phi \vdash$ be $PC^{(\neg, \vee)}$-provable. Then rule (b) yields the provability of $\Gamma, \neg\neg\Phi \vdash$ and Rule 9 yields the $PC^{(\neg, \vee)}$ provability of $\Gamma \vdash \neg\Phi$. We now show that rule (d) is $PC^{(\neg, \vee)}$-admissible. From the $PC^{(\neg, \vee)}$-provable sequent $\Gamma, \Phi \vdash \Psi$ and the axiom $\neg\Psi \vdash \neg\Psi$ we obtain the sequent $\Gamma, \neg\Psi, \Phi \vdash$ using Rules 10 to 12. From the $PC^{(\neg, \vee)}$ admissibility of rule

(c) we obtain the $\mathrm{PC}^{(\neg, \vee)}$ provability of the sequent $\Gamma, \neg\Psi \vdash \neg\Phi$.

Now let

$$D = \frac{D_1; D_2; D_3}{\Gamma \vdash \Psi}$$

be a proof in $\mathrm{PC}^{(\neg)}$ the last passage in which is effected by Rule 6. By the induction hypothesis there are quasi-derivations D_1^*, D_2^* and D_3^* in $\mathrm{PC}^{(\neg, \vee)}$ of the sequents

$$\beta(\Gamma), \beta(\Phi) \vdash \beta(\Psi);$$

$$\beta(\Gamma), \beta(X) \vdash \beta(\Psi) \quad \text{and} \quad \beta(\Gamma) \vdash \neg(\neg\beta(\Phi) \wedge \neg\beta(X))$$

respectively. By the $\mathrm{PC}^{(\neg, \vee)}$ admissibility of rule (d) the following tree will be a quasi-derivation in $\mathrm{PC}^{(\neg, \vee)}$ of the sequent $\beta(\Gamma) \vdash \beta(\Psi)$:

$$\dfrac{\dfrac{\dfrac{D_1^*}{\beta(\Gamma), \neg\beta(\Psi) \vdash \neg\beta(\Phi)} \quad \dfrac{D_2^*}{\beta(\Gamma), \neg\beta(\Psi) \vdash \neg\beta(X)}}{\beta(\Gamma), \neg\beta(\Psi) \vdash \neg\beta(\Phi) \wedge \neg\beta(X); D_3^*}}{\dfrac{\beta(\Gamma), \neg\beta(\Psi) \vdash}{\beta(\Gamma) \vdash \beta(\Psi)}.} \square$$

So far we have treated extensions of the languages of calculi resulting only from extending their alphabets. We now discuss an extension *LG* of the language of $\mathrm{PC}^{(\neg, \vee)}$ whose alphabet and formulas are the same as in $\mathrm{PC}^{(\neg, \vee)}$ but the sequents are defined like this: if Γ and Θ are sequences of formulas of $\mathrm{PC}^{(\neg, \vee)}$, then $\Gamma \vdash \Theta$ is a sequent of the language *LG*.

Now we define the calculus G_0 of the language *LG*. The axioms of G_0 will be sequents of the form $P, \Gamma \vdash \Theta, P$, where P is an atomic formula and Γ, Θ are sequences of atomic formulas. The rules of inference for G_0 will be the following:

$$(1)\ \frac{\Gamma \vdash \Theta, \Phi; \Gamma \vdash \Theta, \Psi}{\Gamma \vdash \Theta, \Phi \wedge \Psi}, \qquad (5)\ \frac{\Gamma \vdash \Delta, \Phi, \Psi, \Theta}{\Gamma \vdash \Delta, \Psi, \Phi, \Theta},$$

$$(2)\ \frac{\Phi, \Psi, \Gamma \vdash \Theta}{\Phi \wedge \Psi, \Gamma \vdash \Theta}, \qquad (6)\ \frac{\Gamma, \Phi, \Psi, \Delta \vdash \Theta}{\Gamma, \Psi, \Phi, \Delta \vdash \Theta},$$

$$(3)\ \frac{\Phi, \Gamma \vdash \Theta}{\Gamma \vdash \Theta, \neg\Phi}, \qquad (7)\ \frac{\Gamma \vdash \Theta, \Phi, \Phi}{\Gamma \vdash \Theta, \Phi},$$

$$(4)\ \frac{\Gamma \vdash \Theta, \Phi}{\neg\Phi, \Gamma \vdash \Theta}, \qquad (8)\ \frac{\Phi, \Phi, \Gamma \vdash \Theta}{\Phi, \Gamma \vdash \Theta},$$

where Φ, Ψ are variables for the formulas of G_0 and Γ, Θ, Δ are variables for the sequences of formulas of G_0.

In the remainder of this section, formulas and sequents, unless otherwise stated, are formulas and sequents of G_0.

LEMMA 1. *Let the sequent* $\Gamma \vdash \Theta$ *be* G_0*-provable and let sequences* Γ_1 *and* Θ_1 *contain among their terms all the terms of the sequences* Γ *and* Θ *respectively. Then the sequent* $\Gamma_1 \vdash \Theta_1$ *is* G_0*-provable.*

PROOF. We show by induction on the length of Φ that for any sequences of formulas Γ and Θ the G_0 provability of the sequent $\Gamma \vdash \Theta$ implies the G_0 provability of the sequents $\Phi, \Gamma \vdash \Theta$ and $\Gamma \vdash \Theta, \Phi$. The statement of the lemma is obtained from Rules (5) to (8).

If Φ is an atomic formula and D is a proof in G_0 of the sequent $\Gamma \vdash \Theta$, then it is obvious that by replacing in D each sequent $\Gamma' \vdash \Theta'$ by $\Gamma', \Phi \vdash \Theta'$ (by $\Gamma' \vdash \Phi, \Theta'$) we obtain a proof in G_0 of the sequent $\Gamma, \Phi \vdash \Theta$ (the sequent $\Gamma \vdash \Phi, \Theta$). Applying rules (5), (6) we obtain the provability of the sequents $\Phi, \Gamma \vdash \Theta$ and $\Gamma \vdash \Theta, \Phi$.

Let $\Phi = \Psi \wedge X$ and let the sequents $X, \Gamma \vdash \Theta$; $\Gamma \vdash \Theta, \Psi$; $\Gamma \vdash \Theta, X$ be G_0-provable. From the induction hypothesis we obtain the provability of $\Psi, X, \Gamma \vdash \Theta$ and using rule (1) we obtain the provability of $\Gamma \vdash \Theta, \Phi$. By means of rule (2) we also obtain $\Phi, \Gamma \vdash \Theta$.

If $\Phi = \neg \Psi$ and the sequents $\Psi, \Gamma \vdash \Theta$; $\Gamma \vdash \Theta, \Psi$ are G_0-provable, then the G_0 provability of the sequents $\Phi, \Gamma \vdash \Theta$ and $\Gamma \vdash \Theta, \Phi$ is obtained using rules (3) and (4). □

LEMMA 2. (a) *If the sequent* $\Gamma \vdash \Theta, \Phi \wedge \Psi$ *is* G_0*-provable, then so are the sequents* $\Gamma \vdash \Theta$ *and* $\Gamma \vdash \Theta, \Psi$.

(b) *If the sequent* $\Phi \wedge \Psi, \Gamma \vdash \Theta$ *is* G_0*-provable, then so is the sequent* $\Phi, \Psi, \Gamma \vdash \Theta$.

(c) *If the sequent* $\Gamma \vdash \Theta, \neg\Phi$ *is* G_0*-provable, then so is the sequent* $\Phi, \Gamma \vdash \Theta$.

(d) *If the sequent* $\neg\Phi, \Gamma \vdash \Theta$ *is* G_0*-provable, then so is the sequent* $\Gamma \vdash \Theta, \Phi$.

PROOF. We prove statement (b). The proof of the other statements is similar and it is left as an exercise to the reader.

A passage in a proof D is said to be *essential* if it is effected by rules different from interchange rules (5), (6). If D is a tree form proof in G_0, then by D^* we denote the tree obtained from D by removing all the sequents beneath the sequent which is the conclusion for the last essential passage in D.

By induction on the number of essential passages in the tree D we shall prove the following statement: if D is a proof in G_0 of the sequent $\Gamma_1, \Phi \wedge \Psi, \Gamma_2 \vdash \Theta$, then there is a proof D_1 of the sequent $\Gamma_1, \Phi, \Psi, \Gamma_2 \vdash \Theta$, the number of essential passages in D_1 being less than that of essential passages in D.

Let D^* be of the following form:

$$\frac{\dfrac{D'}{\Phi, \Psi, \Gamma' \vdash \Theta'}}{\Phi \wedge \Psi, \Gamma' \vdash \Theta'}.$$

Then as the required D_1 it is possible to take some tree D_1 for which

$$D_1^* = \left(\frac{D'}{\Phi, \Psi, \Gamma' \vdash \Theta'}\right)^*.$$

Let D^* be of the following form:

$$\begin{array}{c} D' \\ \hline \Phi \wedge \Psi, \Phi \wedge \Psi, \Gamma' \vdash \Theta' \\ \hline \Phi \wedge \Psi, \Gamma' \vdash \Theta' \end{array}.$$

Denote by n_0 the number of essential passages in D. By the induction hypothesis there is a proof D_2 of the sequent $\Phi, \Psi, \Phi \wedge \Psi, \Gamma' \vdash \Theta'$ with thc number of essential passages $< n_0 - 1$. Again by the induction hypothesis there is a proof D_3 of the sequent $\Phi, \Psi, \Phi, \Psi, \Gamma' \vdash \Theta'$ with the number of essential passages $< n_0 - 2$. As D_1 one may then take a proof of the sequent $\Gamma_1, \Phi, \Psi, \Gamma_2 \vdash \Theta$ such that D_1^* is

$$\begin{array}{c} D_3 \\ \hline \Phi, \Phi, \Psi, \Psi, \Gamma' \vdash \Theta' \\ \hline \Phi, \Psi, \Psi, \Gamma' \vdash \Theta' \\ \hline \Psi, \Phi, \Psi, \Gamma' \cdot\!\vdash \Theta' \\ \hline \Psi, \Psi, \Phi, \Gamma' \vdash \Theta' \\ \hline \Psi, \Phi, \Gamma' \vdash \Theta' \end{array}.$$

It is clear that the number of essential passages in D_1 is less than $n_0 - 2 +$ $+ 2 = n_0$.

Let D^* be of the following form:

$$\dfrac{\dfrac{D'}{\Gamma_1', \Phi \wedge \Psi, \Gamma_2' \vdash \Theta', X_1} \quad \dfrac{D''}{\Gamma_1', \Phi \wedge \Psi, \Gamma_2' \vdash \Theta', X_2}}{\Gamma_1', \Phi \wedge \Psi, \Gamma_2' \vdash \Theta'. X_1 \wedge X_2}.$$

By the induction hypothesis there are proofs D_1' and D_1'' of the sequents $\Gamma_1', \Phi, \Psi, \Gamma_2' \vdash \Theta', X_1$ and $\Gamma_1', \Phi, \Psi, \Gamma_2' \vdash \Theta', X_2$ respectively and the number of essential passages in D_1', D_1'' is less than that in the trees:

$$\frac{D'}{\Gamma_1', \Phi \wedge \Psi, \Gamma_2' \vdash \Theta', X_1}, \quad \frac{D''}{\Gamma_1', \Phi \wedge \Psi, \Gamma_2' \vdash \Theta', X_2}$$

respectively. As the required D_1 we then take a proof of the sequent $\Gamma_1, \Phi, \Psi, \Gamma_2' \vdash \Theta$ such that

$$D_1^* = \frac{D_1'; D_1''}{\Gamma_1', \Phi, \Psi, \Gamma_2' \vdash \Theta', X_1 \wedge X_2}.$$

The other forms of the last essential passage in D are treated similarly. □

LEMMA 3. *If the sequents* $\Gamma \vdash \Theta, \Phi,$ *and* $\Phi, \Gamma' \vdash \Theta'$ *are* G_0*-provable, then the sequent* $\Gamma, \Gamma' \vdash \Theta, \Theta'$ *is* G_0*-provable.*

PROOF. An essential passage in a tree form proof D is a passage by rules different from interchange rules (5) and (6).

Let Φ be an atomic formula. In this case we shall prove the lemma by induction on the number of essential passages in the proof D of the sequent $\Gamma \vdash \Theta, \Phi$. If D has no essential passages, then $\Gamma \vdash \Theta, \Phi$ differs from the axioms only in the interchange of formulas. Hence either $\Phi \in \Gamma$ or $\Psi \in \Gamma$, $\Psi \in \Theta$ for some atomic Ψ. In the former case the provability of $\Gamma, \Gamma' \vdash \Theta, \Theta'$ follows from that of $\Phi, \Gamma' \vdash \Theta'$ and Lemma 1. In the latter case the provability of $\Gamma, \Gamma' \vdash \Theta, \Theta'$ follows from the axiom $\Psi \vdash \Psi$ with the aid of Lemma 1. Let a proof D of the sequent $\Gamma \vdash \Theta, \Phi$ have $n > 0$ essential passages. Let the last essential passage in D be an application of rule (1):

$$\frac{\Gamma_1 \vdash \Theta_1, \Phi, \Theta_2, \Psi; \Gamma_1 \vdash \Theta_1, \Phi, \Theta_2, \mathrm{X}}{\Gamma_1 \vdash \Theta_1, \Phi, \Theta_2, \Psi \wedge \mathrm{X}},$$

where the sequences Γ_1 and $\langle \Theta_1, \Phi, \Theta_2, \Psi \wedge \mathrm{X} \rangle$ are interchanges of the sequences Γ and $\langle \Theta, \Phi \rangle$. Using the interchange rules we obtain from the induction hypothesis the provability of the sequents $\Gamma, \Gamma' \vdash \Theta_1, \Theta_2, \Theta', \Psi$ and $\Gamma, \Gamma' \vdash \Theta_1, \Theta_2, \Theta', \mathrm{X}$. Applying rule (1) and the interchange rules we obtain the provability of the sequent $\Gamma, \Gamma' \vdash \Theta, \Theta'$. The cases of applying the other rules in the last essential passage for an atomic formula Φ are treated similarly.

We continue the proof of the lemma by applying induction on the length of Φ. Let $\Gamma \vdash \Theta, \Phi$ and $\Phi, \Gamma' \vdash \Theta$ be G_0-provable.

If $\Phi = \Psi \wedge \mathrm{X}$, then by Lemma 2 the sequents $\Gamma \vdash \Theta, \Psi$; $\Gamma \vdash \Theta, \mathrm{X}$ and $\Psi, \mathrm{X}, \Gamma' \vdash \Theta'$ are provable. From the induction hypothesis we first obtain the provability of the sequents $\Gamma, \mathrm{X}, \Gamma' \vdash \Theta, \Theta'$ and then that of the sequent $\Gamma, \Gamma, \Gamma' \vdash \Theta, \Theta, \Theta'$. The provability of the sequent $\Gamma, \Gamma' \vdash \Theta, \Theta'$ can now be obtained using structural rules (5) to (8).

If $\Phi = \neg\Psi$, then by Lemma 2 the sequents $\Psi, \Gamma \vdash \Theta$ and $\Gamma' \vdash \Theta', \Psi$ are provable. By the induction hypothesis we get the provability of $\Gamma', \Gamma \vdash \Theta', \Theta$ and hence that of $\Gamma, \Gamma' \vdash \Theta, \Theta'$, too. □

If Θ is a sequence $\Phi_1, \ldots, \Phi_n$ of formulas of the calculus G_0, then by $\neg\Theta$ we shall denote a sequence $\neg\Phi_1, \ldots, \Phi_n$.

LEMMA 4. *If the sequent* $\Gamma \vdash \Theta$ *is* G_0*-provable, then the sequent* $\neg\Theta, \Gamma\vdash$ *is PC-provable.*

PROOF. By induction on the height of the proof D of the sequent $\Gamma \vdash \Theta$ in G_0. It is suggested that the reader should use his experience with the proofs in PC acquired in the preceding sections.

PROPOSITION 4. $\mathrm{PC}^{(\neg, \vee)} < G_0$.

PROOF. If the sequent $\Gamma \vdash \Theta$, where Θ contains at most one term, is G_0-provable, then it follows from Lemma 4 and Proposition 3 that $\Gamma \vdash \Theta$ is $\mathrm{PC}^{(\neg, \vee)}$-provable.

Consider a $\mathrm{PC}^{(\neg, \vee)}$-provable sequent S. By induction on the height of the proof D of the sequent S in $\mathrm{PC}^{(\neg, \vee)}$ we show that S is G_0-provable.

Let D be the axiom $\Phi \vdash \Phi$ for $\mathrm{PC}^{(\neg, \vee)}$. If Φ is an atomic formula, then $\Phi \vdash \Phi$ is an axiom for G_0. If $\Phi = \Psi \wedge \mathrm{X}$ and $\Psi \vdash \Psi$, $\mathrm{X} \vdash \mathrm{X}$ are G_0-provable, then it follows from Lemma 1 and rules (1), (2) that $\Phi \vdash \Phi$ is G_0-provable. If $\Phi = \neg\Psi$ and $\Psi \vdash \Psi$ is G-provable, then it follows from rules (3), (4) and (6) that the sequent $\Phi \vdash \Phi$ is G_0-provable.

Suppose that the height of D is $n > 0$ and for all sequents S' with a proof in $\mathrm{PC}^{(-,\vee)}$ of height $< n$ the G_0 provability of S' is established. If the last passage in D is effected by Rule 1 or 11 for PC, then the G_0 provability of S follows from the induction hypothesis and rules (1) and (6) for G_0.

If D has one of the following forms:

$$\frac{\dfrac{D'}{\Gamma \vdash \Phi \wedge \Psi}}{\Gamma \vdash \Phi}, \quad \frac{\dfrac{D'}{\Gamma \vdash \Phi \wedge \Psi}}{\Gamma \vdash \Psi}, \quad \frac{\dfrac{D'}{\Gamma, \neg \Phi \vdash}}{\Gamma \vdash \Phi},$$

then the G_0 provability of S follows from the induction hypothesis and Lemma 2.

If the last passage in D is effected by Rule 12 for PC, then the G_0 provability of S follows from the induction hypothesis and Lemma 1.

Consider the last of the possible cases, where D has the form

$$\frac{\dfrac{D'}{\Gamma \vdash \Phi;} \quad \dfrac{D''}{\Gamma \vdash \neg\Phi}}{\Gamma \vdash}.$$

By the induction hypothesis and Lemma 2 we obtain the G_0 provability of the sequents $\Gamma \vdash \Phi$ and $\Phi, \Gamma \vdash$. Applying Lemma 3 and rules (6) and (8) yields the G_0 provability of the sequent $\Gamma \vdash$. □

The calculus G_0 is part of the calculus G proposed by Gentzen. In comparison with the calculi we have studied Gentzen calculi are more convenient in analysing and searching for formal proofs. This is accounted for by the main feature of these calculi which, roughly speaking, is that the complexity of formulas may only increase when the rules are applied. The calculus G will be treated at length in Chapter 6. Here we shall only use the above property of the calculus G_0 to obtain the consistency of PC without resorting to the notion of interpretation of a calculus. Indeed, consider the sequent $\vdash Q_0$. It is easy to notice by induction on height that if D is a proof of a sequent S in the calculus G_0 and there is an occurrence of a formula in D containing the logical connective $\wedge$ or $\neg$, then that logical connective must occur in S. Therefore, if the sequent $\vdash Q_0$ is G_0-provable, then it can be obtained from an axiom by means of rules (5) to (8) alone, which is obviously impossible. Hence the calculus G_0 is consistent. Applying Propositions 1 to 4 yields the consistency of PC.

Exercises

1. Show that $\mathrm{PC}^{(-,\wedge)} < \mathrm{PC}$, where $\mathrm{PC}^{(-,\wedge)}$ is obtained from $\mathrm{PC}^{(-)}$ by removing from the alphabet the symbol $\wedge$ and the corresponding rules.

2. Show that $\mathrm{PC}^{(-,\vee,\neg)} < \mathrm{PC}$, where $\mathrm{PC}^{(-,\vee,\neg)}$ is obtained from $\mathrm{PC}^{(-,\vee)}$ by removing from the alphabet the symbol $\neg$ and the corresponding rules. (*Hint*. Use the PC completeness theorem.)

Chapter 2

SET THEORY

10. PREDICATES AND MAPPINGS

All the objects this book studies are sets, although they are named differently: words, symbols, collections, numbers, functions, formulas and so on.

From an intuitive point of view, not all mathematical objects are sets, of course; it is difficult, for example, to think of a parenthesis or a propositional variable as sets. They can be identified with sets, however, by means of suitable conventions (coding). In particular, the parenthesis can be identified with the set $\{\{\varnothing\}\}$. This method is fruitful, and such a convention * is adopted in this book. As the axiom for set theory we admit the *axiom of extensionality* which states that two sets with equal elements are equal; in other words, any set is determined by its elements.

If $a_1, \ldots, a_n$ are all elements of a set A, then by virtue of the axiom of extensionality the set A can be denoted by $\{a_1, \ldots, a_n\}$. It is not assumed that $a_1, \ldots, a_n$ are pairwise distinct. It is clear that the same set A may have many such designations, for example,

$$\{a, b, a\} = \{a, b, b\} = \{a, b\} = \{b, a\}.$$

The sets $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$ and so on (each subsequent set consisting of all the previous ones) are called *natural numbers* and designated respectively 0, 1, 2 and so on. The set of all natural numbers is denoted by ω. Words $\alpha_1 \alpha_2 \ldots \alpha_n$ and finite sequences $\alpha_1, \alpha_2, \ldots, \alpha_n$ will be identified with *ordered collections* $\langle \alpha_1, \ldots, \alpha_n \rangle$ of elements $\alpha_1, \ldots, \alpha_n$ which we shall now define by induction on n.

---

* For some objects, which are not sets from an intuitive point of view, we fix their coding in terms of sets (as for the natural numbers), for others we do not specify their coding since they are not involved in our arguments, the only important thing being separating these objects out among other sets occurring in this book.

DEFINITION. An ordered collection $\langle\ \rangle$ of an empty set of elements is equal to $\varnothing$. An ordered collection $\langle a \rangle$ of one element a is equal to a. An ordered collection $\langle a, b\rangle$ of two elements a and b is called an ordered pair and is $\{\{a\}, \{a, b\}\}$. If $n > 2$, then an ordered collection $\langle a_1, \ldots, a_n\rangle$ of elements $a_1, \ldots, a_n$ is an ordered pair $\langle\langle a_1, \ldots, a_{n-1}\rangle, a_n\rangle$.

An ordered collection $\langle a_1, \ldots, a_n\rangle$ will sometimes be called a *suite* and n will be the length of the suite, $\langle a_1, \ldots, a_n\rangle$, the length of an empty suite $\langle\ \rangle$ being zero. A suite of length $n > 2$ will be called an *ordered n-tuple* or simply an n-tuple (a triple, a quadruple and so on). The identification of words and sequences with ordered collections is possible due to the following proposition.

PROPOSITION 1. *If* $\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle$, *then* $a_1 = b_1, \ldots, a_n = b_n$.

PROOF. It follows from the definition of an ordered collection that it suffices to prove the proposition for $n = 2$. From the condition $\langle a_1, a_2\rangle = \langle b_1, b_2\rangle$ and the definition of an ordered pair we have $\{a_1\} \in \langle b_1, b_2\rangle$. Since $\langle b_1, b_2\rangle = \{\{b_1\}, \{b_1, b_2\}\}$, we have $\{a_1\} = \{b_1\}$ or $\{a_1\} = \{b_1, b_2\}$ and so $b_1 \in \{a_1\}$, i. e. $b_1 = a_1$. It is easy to notice that if $\{x, y\} = \{x, z\}$, then $y = z$. Hence from the obtained equation $\{\{a_1\}, \{a_1, a_2\}\} = \{\{a_1\}, \{a_1, b_2\}\}$ we first get $\{a_1, a_2\} = \{a_1, b_2\}$ and then $a_2 = b_2$. □

DEFINITION. (a) A set $\{\langle a_0, \ldots, a_n\rangle \mid a_0 \in A_0, \ldots, a_n \in A_n\}$ is called a *Cartesian product of sets* $A_0, \ldots, A_n$ and denoted by $A_0 \times \ldots \times A_n$. If $X \subseteq A_0 \times \ldots \times A_n$, then the set of all $a \in A_i$ for which there are $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ such that $\langle a_0, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_n\rangle \in X$ is said to be a projection of X and denoted by $\pi_i^n X$.

(b) If $A_1 = \ldots = A_n = A$, then $A_1 \times \ldots \times A_n$ is said to be the Cartesian n-power of a set A and denoted by A^n. If $n = 0$, then by definition we set $A^0 = \{\varnothing\}$.

(c) Subsets $B \subseteq A^n$ will be called *n-place relations* or *predicates* on A. We shall say that B is an n-place relation or predicate if B is an n-place relation on A for some set A.

(d) If B is a two-place relation, then the two-place relation $\{\langle a, b\rangle \mid \langle b, a\rangle \in B\}$ is said to be the *inverse* of B and denoted by B^{-1}.

(e) If B, C are two two-place relations, then the two-place relation

$$\{\langle a, c\rangle \mid \langle a, b\rangle \in B \quad \text{and} \quad \langle b, c\rangle \in C \text{ for some } b\}$$

is said to be a *composition* or *product* of two-place relations B, C and denoted by (BC) or $B \cdot C$.

Since $\langle a\rangle = a$, we have $A^1 = A$ and so the subsets of A are one-place predicates on A.

Notice that there are only two 0-place predicates, $\varnothing$ and $\{\varnothing\}$. It is immediate from the definition of B^{-1} that $B = (B^{-1})^{-1}$.

PROPOSITION 2. *If B, C and D are two-place predicates, then*

$$((BC)D) = (B(CD)).$$

PROOF. Let $\langle x, y\rangle \in ((BC)D)$. Then for some u and v we have $\langle x, u\rangle \in B$, $\langle u, v\rangle \in C$ and $\langle v, y\rangle \in D$. Thus $\langle u, y\rangle \in (CD)$ and $\langle x, y\rangle \in (B(CD))$. The inclusion $(B(CD)) \subseteq ((BC)D)$ is proved similarly. □

The associativity of a composition, proved in Proposition 2, allows the composition $((BC)D) = (B(CD))$ to be denoted by (BCD). For the same reason, uniquely defined is a composition of n predicates $(B_1, \ldots, B_n)$. Note that the commutativity $(BC) = (CB)$ does not hold for a product of predicates (give an example).

DEFINITION. A two-place relation U on a set A is said to be

(a) a *diagonal* A^2 and denoted by id_A if $U = \{\langle a, a\rangle \mid a \in A\}$;

(b) *reflexive* on A if $\mathrm{id}_A \subseteq U$;

(c) *symmetric* if $U = U^{-1}$;

(d) *transitive* if $(UU) \subseteq U$;

(e) an *equivalence* on A if U is reflexive, symmetric and transitive;

(f) *antisymmetric* if $U \cap U^{-1} \subseteq \mathrm{id}_A$.

For example, the predicate $\{\langle m, n\rangle \mid m$ and n are mutually prime natural numbers$\}$ is symmetric but not reflexive and not transitive on ω and the predicate $\{\langle m, n\rangle \mid (n - m) > 0,$ $n, m \in \omega\}$ is transitive on ω but not symmetric and not reflexive on ω.

If U is an n-place relation on A and $B \subseteq A$, then the relation $U \cap B^n$ on the set B is said to be a *restriction of the relation U to the* *set B*. It is obvious that restrictions of relations of types (a) to (f) in the preceding definition to any $B \subseteq A$ will also be the relations of the corresponding types (a) to (f).

EXAMPLE 1. We say that $R = \{A_i \mid i \in I\}$ is a partition of a set A if $\bigcup_{i \in I} A_i = A$ and for any $i, j \in I$ either $A_i = A_j$ or $A_i \cap A_j = \varnothing$. Let $R = \{A_i \mid i \in I\}$ be a partition of the set A. We define the following two-place relation on A:

$$E_R = \{\langle a, b\rangle \mid a, b \in A_i \quad \text{for some} \quad i \in I\}.$$

It is obvious that E_R is an equivalence on A.

If E is an equivalence on the set A, then the sets $E_x = \{a \mid \langle a, x\rangle \in E\}$ for $x \in A$ will be called *classes of equivalence* with respect to E.

It is easy to show that any equivalence on the set A can be obtained by the method of Example 1. Indeed, let E be an equivalence on A and let $R_E = \{E_x \mid x \in A\}$. It follows from the reflexivity of E that $x \in E_x$, and hence $\bigcup_{x \in A} E_x = A$. It follows from the symmetry and transitivity of E that if $\langle x, y\rangle \in E$, then $E_x = E_y$ and if $\langle x, y\rangle \notin E$, then $E_x \cap E_y = \varnothing$. Thus the set R_E of equivalence classes with respect to E is a partition of A and $E_{R_E} = E$.

DEFINITION. (a) A two-place relation f is said to be a *mapping* or *function* if for any a, b, c in $\langle a, b\rangle \in f$ and $\langle a, c\rangle \in f$ we have $b = c$. If f is a mapping, then the set $\pi_1^2 f$ is said to be the *domain* of f and denoted by $\operatorname{dom} f$ and the set $\pi_2^2 f$ is said to be the *range* of f and denoted by $\operatorname{rang} f$.

(b) A mapping f is said to be *distinct-valued* if f^{-1} is also a mapping.

(c) A mapping f is said to be a mapping of A *into* B if $\operatorname{dom} f = A$ and $\operatorname{rang} f \subseteq B$.

(d) A mapping f is said to be a mapping of A *onto* B if $\operatorname{dom} f = A$ and $\operatorname{rang} f = B$.

(e) A mapping f of a set A^n into A is said to be an *n-place operation* on A.

It is obvious that the diagonal id_A of the set A^2 will be a distinct-valued one-place operation on A. The diagonal id_A of the set A^2 will also be called an identity operation on A in what follows.

The notation $f\colon A \to B$ will designate in the sequel that f is a mapping of A into B and the notation $f\colon A \twoheadrightarrow B$ will designate that f is a mapping of A onto B.

PROPOSITION 3. (a) *If* $f\colon A \to B$ *and* $g\colon B \to C$, then $(fg)\colon A \to C$.

(b) *If* $f\colon A \twoheadrightarrow B$ *and* $g\colon B \twoheadrightarrow C$, *then* $(fg)\colon A \twoheadrightarrow C$.

(c) *If* f *is a distinct-valued mapping of* A *onto* B, *then* f^{-1} *is a distinct-valued mapping of* B *onto* A, $f\cdot f^{-1} = \mathrm{id}_A$ *and u*$f^{-1}\cdot f = = \mathrm{id}_B$.

(d) *If* f *and* g *are distinct-valued mappings, then* $f\cdot g$ *is also distinct-valued and* $(fg)^{-1} = (g^{-1}f^{-1})$.

The proof of this proposition is left as an exercise to the reader. □

If f is a mapping and $\langle a, b\rangle \in f$, then b is said to be the *value of* f *at the element* a and denoted by $f(a)$ or fa.

If f is a mapping and $A \subseteq \operatorname{dom} f$, then the set $\{fa \mid a \in A\}$ is said to be the *image of a set* A *under the mapping* f and denoted by $f[A]$ and the mapping $f \cap (A \times \operatorname{rang} f)$ is said to be the *restriction* of f to A and denoted by $f \restriction A$.

It is clear that an n-place operation is an $(n + 1)$-place relation and the 0-place operation $f\colon A^0 \to A$ is $\{\langle \varnothing, a\rangle\}$ for some $a \in A$. The 0-place operation $\{\langle \varnothing, a\rangle\}$ on A will often be called a constant on A and identified with the element a.

If f is an n-place operation on A, then the condition $\langle a_1, \ldots, a_n, b\rangle \in f$ will be written as: $f(a_1, \ldots, a_n) = b$. For $n = 0$ this will be $f(\,) = b$, i. e. $f = b$, which agrees with the adopted identification of a constant with its value.

If f is an n-place operation on A and $B \subseteq A$, then the set B is said to be *closed under the operation* f when $a_1, \ldots, a_n \in B$ implies $f(a_1, \ldots, a_n) \in B$.

Exercises

1. Suppose U is a transitive two-place relation on a set A, $(a, a) \notin U$ for any a and for any $a \in A$ there is b such that $\langle a, b\rangle \in U$. Show that A is finite.

2. Prove Proposition 3.

3. If $f\colon A \to B$, $g\colon B \twoheadrightarrow A$ and $(gf) = \mathrm{id}_B$, then f is distinct-valued and $g = f^{-1}$.

11. PARTIALLY ORDERED SETS

Among the various types of relations some are of fundamental importance not only for mathematical logic but also for the whole of mathematics. In the preceding section we have already treated one of such relations, that of equivalence. Now we define another two very important types of relations.

DEFINITION. (a) A relation U on a set A is said to be a *partial ordering on A* if it is reflexive, transitive and antisymmetric.

(b) A partial ordering U on A is said to be a *linear ordering on A* if at least one of the following conditions: $\langle a, b\rangle \in U$, $\langle b, a\rangle \in U$ or $a = b$ holds for any $a, b \in A$.

It is obvious that restriction of a partial (linear) ordering on A to any subset $B \subseteq A$ is a partial (linear) ordering on B.

An important example of a partial ordering on the set A is the relation $\{\langle a, b\rangle | a, b \in A, a \subseteq b\}$ and an example of a linear ordering is the relation $\{\langle a, b\rangle | a, b \in X, a \leqslant b\}$, where X is some subset of the real numbers.

DEFINITION. (a) If U is a partial ordering on A, then the pair $\mathfrak{A} = \langle A, U\rangle$ is said to be a *partially ordered set* (abbreviated poset).

(b) If U is a linear ordering on A, then the pair $\mathfrak{A} = \langle A, U\rangle$ is said to be a *linearly ordered set*.

Let $\mathfrak{A} = \langle A, U\rangle$ be a partially ordered set. The element $a_0 \in A$ is said to be the *upper* (*lower*) *bound in* $\mathfrak{A}$ of a subset $A_0 \subseteq A$ if $\langle b, a_0\rangle \in U$ ($\langle a_0, b\rangle \in U$) for all $b \in A_0$. The upper (lower) bound in $\mathfrak{A}$ of A is the *greatest* (*least*) element in $\mathfrak{A}$. An element $a \in A$ is said to be *maximal* (*minimal*) in $\mathfrak{A}$ if $\langle a, x\rangle \in U$ (respectively $\langle x, a\rangle \in U$) implies $x = a$. It is clear that the greatest (least) element is maximal (minimal), and if U is a linear ordering, then the element maximal (minimal) in $\mathfrak{A}$ is also the greatest (least) in $\mathfrak{A}$. It is obvious that if the greatest (least) element in $\mathfrak{A}$ exists, then all the maximal (minimal) elements are equal.

If B is a set of upper bounds in $\mathfrak{A} = \langle A, U\rangle$ of a set $A_1 \subseteq A$, then the least element in $\langle B, U \cap B^2\rangle$ is said to be the *least upper bound* (abbreviated lub) in $\mathfrak{A}$ of the set A_1 and denoted $\sup(A_1, \mathfrak{A})$. Replacing in the preceding definition "upper" and "least" respectively by "lower" and "greatest" we obtain the definition of the *greatest lower bound* (abbreviated glb) of A_1 in $\mathfrak{A}$ which will be denoted by inf $(A_1, \mathfrak{A})$. It is clear that sup $(A_1, \mathfrak{A})$ and inf $(A_1, \mathfrak{A})$ are uniquely determined by A_1 and $\mathfrak{A}$ if they exist.

DEFINITION. A partially ordered set $\mathfrak{A} = \langle A, U\rangle$ is said to be a *lattice* if for any $a, b \in A$ in $\mathfrak{A}$ there are sup $(\{a, b\}, \mathfrak{A})$, and inf $(\{a, b\}, \mathfrak{A})$ which will be denoted by $a \cup^{\mathfrak{A}} b$ and $a \cap^{\mathfrak{A}} b$. A lattice $\mathfrak{A} = \langle A, U\rangle$ is said to be *distributive* if for any $a, b, c \in A$ the operations $\cup^{\mathfrak{A}}$ and $\cap^{\mathfrak{A}}$ satisfy the following conditions:

$$\text{(D)}\quad a \cup^{\mathfrak{A}} (b \cap^{\mathfrak{A}} c) = (a \cup^{\mathfrak{A}} b) \cap^{\mathfrak{A}} (a \cup^{\mathfrak{A}} c);$$

$$\text{(D}'\text{)}\quad a \cap^{\mathfrak{A}} (b \cup^{\mathfrak{A}} c) = (a \cap^{\mathfrak{A}} b) \cup^{\mathfrak{A}} (a \cap^{\mathfrak{A}} c);$$

The lattice $\mathfrak{A} = \langle A, U\rangle$ is said to be a *Boolean lattice* if $\mathfrak{A}$ is distributive, has the greatest element $1^{\mathfrak{A}}$ and the least element $0^{\mathfrak{A}}$, $0^{\mathfrak{A}} \neq 1^{\mathfrak{A}}$ and for any $a \in A$ there is an element $\bar{a} \in A$ such that $\bar{a} \cup^{\mathfrak{A}} a = 1^{\mathfrak{A}}$ and $\bar{a} \cap^{\mathfrak{A}} a = 0^{\mathfrak{A}}$. An element $\bar{a}$ satisfying in the lattice $\mathfrak{A}$ with the greatest element $1^{\mathfrak{A}}$ and the least element $0^{\mathfrak{A}}$ the above conditions is called a *complement of the element a* in $\mathfrak{A}$.

PROPOSITION 1. (a) *If a complement a of an element a in a distributive lattice* $\mathfrak{A}$ *with the greatest and the least element exists, then it is unique.*

(b) *If* $\mathfrak{A} = \langle A, U\rangle$ *is a Boolean lattice, then for any* $a, b, c \in A$ *the operations* $\cup^{\mathfrak{A}}$, $\cap^{\mathfrak{A}}$ *and* $^-$ *defined above satisfy the following conditions* (*with the superscript* $\mathfrak{A}$ *in* $\cup^{\mathfrak{A}}$ *and* $\cap^{\mathfrak{A}}$ *omitted for simplicity*):

(1) $a \cup b = b \cup a,$
(2) $a \cap b = b \cap a,$
(3) $a \cup (b \cup c) = (a \cup b) \cup c,$
(4) $a \cap (b \cap c) = (a \cap b) \cap c,$
(5) $(a \cap b) \cup b = b,$
(6) $(a \cup b) \cap b = b,$
(7) $a \cap (b \cup c) = (a \cap b) \cup (a \cap c),$
(8) $a \cup (b \cap c) = (a \cup b) \cap (a \cup c),$
(9) $(a \cap \bar{a}) \cup b = b$
(10) $(a \cup \bar{a}) \cap b = b.$

(c) *If on a set A we are given three operations,* $\cup$, $\cap$ *and* $^-$, *satisfying for any* $a, b, c \in A$ *conditions* (1) *to* (10) *of statement* (b) (*where* $\cup (a, b)$, $\cap (a, b)$ and $^{-}(a)$ *are written as* $a \cup b$, $a \cap b$, and $\bar{a}$), *then the pair* $-\mathfrak{A} = \langle A, U\rangle$ *for* $U = \{\langle a, b\rangle | a \cap b = a\}$ *is a Boolean lattice, with* $a \cup b = \sup(\{a, b\}, \mathfrak{A})$, $a \cap b = \inf(\{a, b\}, \mathfrak{A})$, $\bar{a} \cup a = 1^{\mathfrak{A}}$, $\bar{a} \cap a = 0^{\mathfrak{A}}$.

PROOF. (a) The superscript $\mathfrak{A}$ in $\cup^{\mathfrak{A}}$, $\cap^{\mathfrak{A}}$, $1^{\mathfrak{A}}$, and $0^{\mathfrak{A}}$ will be omitted for simplicity. If $a \cup a_1 = 1$ and $a \cap a_2 = 0$, then

$$a_1 = a_1 \cup 0 = a_1 \cup (a \cap a_2) = (a_1 \cup a) \cap (a_1 \cup a_2) = \\ = 1 \cap (a_1 \cup a_2) = a_1 \cup a_2.$$

Similarly, from $a \cap a_1 = 0$ and $a \cup a_2 = 1$ we get $a_2 = a_2 \cup a_1$, hence $a_1 = a_2$.

(b) Properties (1) and (2) are obvious. Since $a \cap \bar{a} = 0^{\mathfrak{A}}$ and $a \cup \bar{a} = 1^{\mathfrak{A}}$, properties (9) and (10) hold. Since $\mathfrak{A}$ is distributive, (7) and (8) hold. In what follows the condition $\langle a, b\rangle \in U$ is denoted by $a \leqslant b$. It follows from the definition of the operations $\cup^{\mathfrak{A}}$ and $\cap^{\mathfrak{A}}$ that for any $d, m_1, m_2 \in A$

(1) $d \leqslant m_1 \cap m_2 \Leftrightarrow (d \leqslant m_1$ and $d \leqslant m_2)$,
(2) $m_1 \cup m_2 \leqslant d \Leftrightarrow (m_1 \leqslant d$ and $m_2 \leqslant d)$,
(3) $m_1, m_2 \leqslant m_1 \cup m_2$,
(4) $m_1 \cap m_2 \leqslant m_1, m_2$.

Using these facts it is easy to establish properties (3) to (6). We check, for example, property (6), leaving the rest to the reader. From (4) we get $(a \cup b) \cap b \leqslant b$ and from (3) and (1) we get $b \leqslant (a \cup b) \cap b$, hence from the antisymmetry of U, we get (6).

(c) From conditions (5), (6), (1) and (2) we get

$$a \cap b = a \Leftrightarrow a \cup b = b. \tag{*}$$

We first show that $U = \{\langle a, b\rangle | a \cap b = a\}$ is a partial ordering. Substituting in (7) an element a for b and an element $\bar{a}$ for c and using conditions (2), (1), (6) and (9) we get $a = a \cap a$, hence U is reflexive. Let $a \cap b = a$ and $b \cap c = b$. From (*), (7), (5), (1) and (2) we get

$$a \cap c = a \cap (b \cup c) = (a \cap b) \cup (a \cap c) = a \cup (a \cap c) = a.$$

Hence U is transitive. Let $a \cap b = a$ and $b \cap a = b$. Then from (2) we get $a = b$, i. e. U is antisymmetric. To complete the proof it is necessary to show that $a \cup b = \sup(\{a, b\}, \mathfrak{A})$ and $a \cap b = \inf(\{a, b\}, \mathfrak{A})$. We prove the first of the equations, leaving the second for the reader to check. From

$$a \cap (a \cup b) = (a \cap a) \cup (a \cap b) = a \cup (a \cap b) = a$$

and $a \cup b = b \cup a$ it follows that $a \cup b$ is the upper bound of the set $\{a, b\}$. Let c be the upper bound of $\{a, b\}$, i. e. $a \cap c = a$ and $b \cap c = b$. Then

$$(a \cup b) \cap c = c \cap (a \cup b) = (c \cap a) \cup (c \cap b) = a \cup b,$$

i. e. $\langle a \cup b, c\rangle \in U$. □

Conditions (1) to (10) of Proposition 1 are called axioms of Boolean algebras and the set A, together with the operations $\cap$, $\cup$, and $^-$ defined on it and satisfying axioms (1) to (10) is a *Boolean algebra.* If $\mathfrak{A} = \langle A, \cup, \cap, ^- \rangle$ is a Boolean algebra, then $\leqslant$ will denote a partial ordering on A defined by the condition

$$a \leqslant b \Leftrightarrow a \cap b = a.$$

From Proposition 1 it follows that the Boolean algebra is uniquely determined by the relation $\leqslant$.

EXAMPLES. (1) If $A \subseteq P(B)$ and the set A is closed under the operations of union and intersection, then it is easy to verify that $\mathfrak{A} = \langle A, \subseteq \rangle$, where $\subseteq$ is the inclusion relation on A, is a distributive lattice, with $\cup^{\mathfrak{A}}$ and $\cap^{\mathfrak{A}}$ being the union and intersection operations on A.

(2) If in example (1) the set A is closed under the complement operation in B, i. e. the operation $\bar{a} = B \setminus a$, then $\mathfrak{A} = \langle A, \subseteq \rangle$ is a Boolean lattice and $\langle A, \cup, \cap, ^- \rangle$ is a Boolean algebra, where $\cup$, $\cap$, $^-$ are the union, intersection and complement operations in B. In particular, if $A = P(B)$, then $\langle P(B), \cup, \cap, ^- \rangle$ is said to be the *Boolean algebra of all subsets of B* and for simplicity it will be denoted by the same symbol $P(B)$ as the set of all subsets of B.

DEFINITION. A partially ordered set $\mathfrak{A} = \langle A, U\rangle$ is said to be *well-founded* if for any nonempty subset $A_1 \subseteq A$ the poset $\mathfrak{A}_1 = \langle A_1, U \cap A_1^2\rangle$ has a minimal element.

If $\langle A, U\rangle$ is a well-founded partially ordered set, then obviously $\langle B, U \cap B^2\rangle$ is also a well-founded partially ordered set for any $B \subseteq A$.

It is possible to extend the method of mathematical induction to a well-founded partially ordered set.

PROPOSITION 2 (Principle of Transfinite Induction). *Let* $\mathfrak{A} = \langle A, U\rangle$ *be a well-founded partially ordered set and* $B \subseteq A$. *If for any* $a \in A$, *from* $\{b \in A \mid \langle b, a\rangle \in U, b \neq a\} \subseteq B$ *we have* $a \in B$, *then* $B = A$.

PROOF. Suppose that $B \neq A$ and let a_0 be the minimal element of a poset $\langle A \setminus B, U \cap (A \setminus B)^2\rangle$. Then $\{b \in A \mid \langle b, a_0\rangle \in U, b \neq a_0\} \subseteq B$ and under the hypothesis we have $a_0 \in B$, which is impossible. □

DEFINITION. Let $\mathfrak{A} = \langle A, U\rangle$ be a linearly ordered set. The set $X \subseteq A$ is said to be

(a) the *initial segment* of $\mathfrak{A}$ if for any $a, b \in A$, from $a \in X$ and $\langle b, a\rangle \in U$ we have $b \in X$;

(b) a *closed initial segment* if for some $a_0 \in A$ X is the set $O[a_0, \mathfrak{A}] = \{b \mid \langle b, a_0\rangle \in U\}$;

(c) an *open initial segment* if X is equal to the set $O(a_0, \mathfrak{A}) = (O[a_0, \mathfrak{A}] \setminus \{a_0\})$ for some $a_0 \in A$.

We shall often write $O[a_0]$ and $O(a_0)$ instead of $O[a_0, \mathfrak{A}]$ and $O(a_0, \mathfrak{A})$, respectively, when it is clear what $\mathfrak{A}$ is meant. Notice that the empty set $\varnothing$ is the initial segment of any linearly ordered set. It is obvious that the element a_0 in (b) and (c) of the preceding definition is uniquely defined by X.

EXAMPLES. Let G be the "less than or equal to" relation on real numbers (i. e. $\langle a, b\rangle \in G \Leftrightarrow a \leqslant b$).

1. In the linearly ordered set $\langle \omega, G \cap \omega^2\rangle$ any initial segment other than ω is at once open and closed.

2. In $\langle R, G\rangle$ where R is the set of all real numbers, any initial segment other than R is open or closed, but none of the initial segments of $\langle R, G\rangle$ is at once open and closed.

3. In $\langle Q, G \cap Q^2\rangle$, where Q is the set of all rational numbers, the initial segment $\{r \mid r < \sqrt{2}\}$ is neither open nor closed.

DEFINITION. If $\mathfrak{A} = \langle A, U\rangle$ is a well-founded linearly ordered set, then $\mathfrak{A}$ is said to be a *well-ordered set*. If $\mathfrak{A} = \langle A, U\rangle$ is a poset, $X \subseteq A$ and $U \cap X^2$ is a linear ordering on X, then X is said to be a *chain in* $\mathfrak{A}$. In particular, the empty set is a chain in any poset.

In Section 10 we formulated one axiom of the set theory which we have already used, the axiom of extensionality. Henceforth we shall also use the *axiom of choice* which says that for any nonempty set A there is a mapping (a function of choice) h: $(P(A) \setminus \{\varnothing\} \to A$ such that $h(B) \in B$ for any nonempty set $B \subseteq A$. This axiom yields the following two important principles.

THEOREM 1 (Maximum Principle). *If in a partially ordered set* $\mathfrak{A} = \langle A, U \rangle$ *each chain* $X \subseteq A$ *has an upper bound, then there is an element maximal in* $\mathfrak{A}$.

PROOF. Consider the set $Y = \{X \subseteq A \mid X \text{ is a chain in } \mathfrak{A}\}$ and for $X \in Y$ the set $B(X) = \{a \in A \mid a \text{ is the upper bound of } X \text{ in } \mathfrak{A}\}$. Suppose that $\mathfrak{A}$ has no maximal elements. Then the family $S = \{B(X) \setminus X \mid X \in Y\}$ consists of nonempty subsets of A. It follows from the axiom of choice that there is a mapping h of the set Y into A such that $h(X) \in (B(X) \setminus X)$ for all $X \in Y$. In what follows the initial segment of a linearly ordered set $\langle X, U \cap X^2 \rangle$ will be called the initial segment of X. Consider the set $Z \subseteq Y$ of all nonempty chains X in $\mathfrak{A}$ satisfying the following condition: $h(X_1) = \inf (X \setminus X_1, \langle X, U \cap X^2 \rangle)$ for any initial segment $X_1 \subseteq X$, $X_1 \neq X$. It is obvious that $\{h(\varnothing) \in Z$. Let X_1, $X_2 \in Z$. Since $h(\varnothing)$ is the least element in $\langle X_1, U \cap X_1^2 \rangle$ and $\langle X_2, U \cap X_2^2 \rangle$, X_1 and X_2 have nonempty initial segments in common. Let C be the union of common initial segments of X_1 and X_2. It is clear that C is the initial segment of X_1 and X_2. Then $C = X_1$ or $C = X_2$, since otherwise $C \cup \{h(C)\} \neq C$ would be a common initial segment of X_1 and X_2, which contradicts the definition of C. Thus for any $X_1, X_2 \in Z$ either $X_1 \subseteq X_2$ or $X_2 \subseteq X_1$. Hence $C^* = \bigcup_{X \in Z} X$ is a chain in $\mathfrak{A}$ and $C^* \cup \{h(C^*)\} \in Z$, which contradicts the definition of C^* and the condition $h(C^*) \in B(C^*) \setminus C^*$. □

THEOREM 2 (Principle of Well Ordering). *Every set* A *may be well-ordered, i. e. for every set* A *there is* $U \subseteq A^2$ *for which* $\mathfrak{A} = \langle A, U \rangle$ *is a well-ordered set.*

PROOF. Consider a set $W = \{\langle X, U \rangle \mid \langle X, U \rangle \text{ is a well-ordered set}, X \subseteq A\}$.

We define on the set W an ordering $\preccurlyeq$:

$$\langle X_1, U_1 \rangle \preccurlyeq \langle X_2, U_2 \rangle \Leftrightarrow U_1 \subseteq U_2 \text{ and } X_1 \text{ is the initial segment of } \langle X_2, U_2 \rangle.$$

Let $\{\langle X_i, U_i\rangle \mid i \in I\}$ be a chain in $\langle W, \leqslant\rangle$. It is obvious that $\mathfrak{A} = \left\langle \bigcup_{i\in I} X_i, \bigcup_{i \in I} U_i \right\rangle$ *is a linearly ordered set*. Let $Y \subseteq \bigcup_{i\in I} X_i$ and $Y \neq \varnothing$. Then $Y \cap X_{i_0} \neq \varnothing$ for some $i_0 \in I$. Since $\langle X_{i_0}, U_{i_0}\rangle$ is a well-ordered set, $\langle Y \cap X_{i_0}, U_{i_0} \cap Y^2\rangle$ has a minimal element y_0. Since X_{i_0} is an initial segment of $\mathfrak{A}$, y_0 is a minimal element of $\left\langle Y, \left(\bigcup_{i\in I} U_i\right) \cap Y^2\right\rangle$. Thus $\mathfrak{A} \in W$. It is clear that $\mathfrak{A}$ is an upper bound for the chain $\{\langle X_i, U_i\rangle \mid i \in I\}$ in $\langle W, \leqslant\rangle$. Therefore, by Theorem 1 $\langle W, \leqslant\rangle$ has a maximal element $\langle A_0, U_0\rangle$. If there is $a_0 \in A \setminus A_0$, then $\langle A_0 \cup \{a_0\}, U_1\rangle \in W$, where $U_1 = U_0 \cup \cup \{\langle a, a_0\rangle \mid a \in A_0\} \cup \{\langle a_0, a_0\rangle\}$, which contradicts the maximality of $\langle A_0, U_0\rangle$ in $\langle W, \leqslant\rangle$. Thus $\langle A, U_0\rangle$ is a well-ordered set. □

DEFINITION. Let $\mathfrak{A} = \langle A, U\rangle$ and $\mathfrak{B} = \langle B, V\rangle$ be two linearly ordered sets. A mapping $f\colon A \twoheadrightarrow B$ is said to be a *similarity* of $\mathfrak{A}$ onto $\mathfrak{B}$ if

$$\langle a, b\rangle \in U \Leftrightarrow \langle fa, fb\rangle \in V. \tag{1}$$

We shall say that $\mathfrak{A}$ and $\mathfrak{B}$ are similar if there is a similarity of one of them onto the other.

Notice that the similarity $f\colon A \twoheadrightarrow B$ is distinct-valued. Indeed, if $fa = fb$, then from the reflexivity of V and (1) we get $\langle a, b\rangle \in U$ and $\langle b, a\rangle \in U$ and hence from the antisymmetry of U we get $a = b$. If f is a similarity of $\mathfrak{A}$ onto $\mathfrak{B}$, then it is obvious that f^{-1} is a similarity of $\mathfrak{B}$ onto $\mathfrak{A}$.

PROPOSITION 3. *If f is a similarity of a linearly ordered set $\mathfrak{A}$ onto a linearly ordered set $\mathfrak{B}$ and X is an (open, closed) initial segment of $\mathfrak{A}$, then $f(X)$ is an (open, closed) initial segment of $\mathfrak{B}$.*

The proof is left as an easy exercise to the reader. □

In the remainder of this section we shall prove important properties of well-ordered sets.

PROPOSITION 4. *Any initial segment X of a well-ordered set $\mathfrak{A} = \langle A, U\rangle$ other than A is open.*

PROOF. It is obvious that $X = O(a_0, \mathfrak{A})$, where a_0 is the minimal element of the set $A \setminus X$. □

If X and Y are the initial segments of the linearly ordered sets $\mathfrak{A} = \langle A, U\rangle$ and $\mathfrak{B} = \langle B, V\rangle$ respectively and $\langle X, U \cap X^2\rangle$ is similar to $\langle Y, V \cap Y^2 \rangle$, then in what follows we shall simply say that X is similar to Y.

PROPOSITION 5. *If $f: A \to B$ and $g: A \to B$ are two similarities of a well-ordered set $\mathfrak{A} = \langle A, U \rangle$ onto some initial segments of a linearly ordered set $\mathfrak{B} = \langle B, V \rangle$, then $f = g$.*

PROOF. Consider a set $Q = \{a \in A \mid fa = ga\}$. If $O(b, \mathfrak{A}) \subseteq Q$, then $fb = \inf(B \setminus g[O(b, \mathfrak{A})], \mathfrak{B})$, hence $fb = gb$. By Proposition 2 we have $Q = A$, and Proposition 5 is thus proved. □

PROPOSITION 6. *No two distinct initial segments of a well-ordered set $\mathfrak{A}$ are similar to each other.*

PROOF. Let f be a similarity of an initial segment X onto an initial segment Y. Since id_X is a similarity of X onto X, by Proposition 5 $f = \mathrm{id}_X$, hence $X = Y$. □

THEOREM 3. *If $\mathfrak{A} = \langle A, U \rangle$ and $\mathfrak{B} = \langle B, V \rangle$ are well-ordered sets, then either $\mathfrak{A}$ is similar to the initial segment of $\mathfrak{B}$ or $\mathfrak{B}$ is similar to the initial segment of $\mathfrak{A}$.*

PROOF. Consider a set $P = \{f \mid f$ is a similarity of some initial segment of $\mathfrak{A}$ onto the initial segment of $\mathfrak{B}\}$.

By Propositions 3 and 5, for any $f, g \in P$ either $f \subseteq g$ or $g \subseteq f$. Therefore, $F = \bigcup_{f \in P} f$ is a similarity of the initial segment X of the set $\mathfrak{A}$ onto the initial segment Y of the set $\mathfrak{B}$. If $X = A$ or $Y = B$, then everything is proved. Suppose that this is not the case. Then by Proposition 4 $X = O(a_0, \mathfrak{A})$ and $Y = O(b_0, \mathfrak{B})$. It is obvious that $F \cup \{\langle a_0, b_0 \rangle\}$ is then a similarity of the initial segment $O[a_0, \mathfrak{A}]$ onto the initial segment $O[b_0, \mathfrak{B}]$, hence $F \cup \{\langle a_0, b_0 \rangle\} \subseteq F$, which is impossible.

Exercises

1. Show that if $\mathfrak{A} = \langle A, U \rangle$ is a poset with a least element A is finite and for any $a, b \in A$ there is $\sup(\{a, b\}, \mathfrak{A})$, then $\mathfrak{A}$ is a lattice.

2. Let $\mathfrak{A} = \langle A, \cup, \cap, ^- \rangle$ be a Boolean algebra and let A contain more than one element. The mapping γ of the set F of the formulas of PC in A having the properties:

(1) $\gamma(\Phi \vee \Psi) = \gamma(\Phi) \cup \gamma(\Psi)$,
(2) $\gamma(\Phi \wedge \Psi) = \gamma(\Phi) \cap \gamma(\Psi)$,
(3) $\gamma(\Phi \to \Psi) = \overline{\gamma(\Phi)} \cup \gamma(\Psi)$,
(4) $\gamma(\neg \Phi) = \overline{\gamma(\Phi)}$

is called an interpretation of PC in $\mathfrak{A}$. Show that PC-provable formulas are precisely Φ such that $\gamma(\Phi) = 1^{\mathfrak{A}}$ for any interpretation γ of PC in $\mathfrak{A}$. (*Hint*. In one direction, establish $\gamma(\Phi) = 1^{\mathfrak{A}}$ for the axioms of PC_1 and verify that the rule for PC_1 preserves this property; in the other direction, use the fact that on the set $\{1^{\mathfrak{A}}, 0^{\mathfrak{A}}\}$ the operations $\cup$, $\cap$ and $^{-}$ are defined in the same way as the operations, $\vee$, $\wedge$ and $\neg$ are on the set $\{1, 0\}$ in Sec. 6.)

3. Show that a poset $\langle A, U\rangle$ is not well-founded if and only if there is a sequence $a_0, \ldots, a_n, \ldots$ of pairwise distinct elements of A for which $\langle a_{n+1} a_n\rangle \in U$, $n \in \omega$.

12. FILTERS OF BOOLEAN ALGEBRA

Let $\mathfrak{B} = \langle B, \cap, \cup, ^{-}\rangle$ be a Boolean algebra throughout this section. As shown in Proposition 11.1, $\mathfrak{B}^* = \langle B, \leqslant\rangle$, where the relation $a \leqslant b$ is defined by the equation $a \cap b = a$, is a Boolean lattice and for any $a, b \in B$ the following conditions hold:

(1) $a \cup b = \sup(\{a, b\}, \mathfrak{B}^*)$, $a \cap b = \inf(\{a, b\}, \mathfrak{B}^*)$;

(2) $a \cup \overline{a} = 1$ is the greatest element of $\mathfrak{B}^*$;

(3) $a \cap \overline{a} = 0$ is the least element of $\mathfrak{B}^*$;

(4) $\overline{a}$ is the only element of B for which: $a \cup \overline{a} = 1$ and $a \cap \overline{a} = 0$.

Note some other properties of Boolean operations.

LEMMA 1. (a) $\overline{0} = 1$, $\overline{1} = 0$;

(b) $0 \cap a = 0$, $0 \cup a = a$;

(c) $1 \cap a = a$, $1 \cup a = 1$;

(d) $a = a$;

(e) $\overline{a \cap b} = \overline{a} \cup \overline{b}$;

(f) $\overline{a \cup b} = \overline{a} \cap \overline{b}$;

(g) $a \cap b = a \Leftrightarrow a \cup b = b$.

PROOF. Property (a) follows immediately from (1) to (4). Properties (b), (c) follow from (1) to (3) and property (d) follows from (4) since $\overline{a} \cup a = a \cup \overline{a} = 1$ and $\overline{a} \cap a = a \cap \overline{a} = 0$. Property (g) follows from (1), since $a \cap b = a \Leftrightarrow a \leqslant b$. To prove (e) it suffices by virtue of (4) to show that

$$(a \cap b) \cup (\overline{a} \cup \overline{b}) = 1 \quad \text{and} \quad (a \cap b) \cap (\overline{a} \cup \overline{b}) = 0.$$

These equations follow from axioms (1) to (6) for Boolean algebras, for example,

$$(a \cap b) \cap (\overline{a} \cup \overline{b}) = ((a \cap b) \cap \overline{a}) \cup ((a \cap b) \cap \overline{b}) =$$
$$= (0 \cap b) \cup (0 \cap a) = 0.$$

The verification of the other equation, as well as the proof of property (f), is similar. ☐

We shall often identify $\mathfrak{B}^*$ with $\mathfrak{B}$ for notational simplicity.

DEFINITION. A set $D \subseteq B$ is said to be a *filter of a Boolean algebra* $\mathfrak{B}$ if the following conditions hold:

(1) $0 \notin D$,

(2) if $a, b \in D$, then $a \cap b \in D$;

(3) if $a \in D$ and $a \leqslant b$, then $b \in D$.

A set $D \subseteq P(X)$ is said to be a *filter on a set X* if D is a filter of the Boolean algebra $\langle P(X), \cup, \cap, {}^- \rangle$

EXAMPLES. 1. The set $\{1\}$ is a filter of the Boolean algebra $\mathfrak{B}$. On the other hand, it follows from condition (3) that $1 \in D$ for any nonempty filter D in the Boolean algebra $\mathfrak{B}$.

2. If $a_0 \in B$, $a_0 \neq 0$, then the set $\{b \mid b \in B, a_0 \leqslant b\}$ is a filter of the algebra $\mathfrak{B}$.

3. The set $\{Y \subseteq X \mid (X \setminus Y)$ is a finite set$\}$ is a filter on X, sometimes called a Fréchet filter on X.

Since the operations $\cup$ and $\cap$ of the Boolean algebra $\mathfrak{B}$ satisfy the axioms of commutativity (1), (2) and the axioms of associativity (3), (4), one may speak of the union and intersection in $\mathfrak{B}$ of a finite set of elements $a_1, \ldots, a_n \in B$ and designate it as: $a_1 \cup \ldots \cup a_n$ ($a_1 \cap \ldots \cap a_n$). It is easy to establish by induction on n the following generalized distributive laws:

$$b \cup (a_1 \cap \ldots \cap a_n) = (b \cup a_1) \cap \ldots \cap (b \cup a_n),$$

$$b \cap (a_1 \cup \ldots \cup a_n) = (b \cap a_1) \cup \ldots \cup (b \cap a_n)$$

and generalized properties (e), (f) of Lemma 1:

$$\overline{a_1 \cap \ldots \cap a_n} = \bar{a}_1 \cup \ldots \cup \bar{a}_n,$$

$$\overline{a_1 \cup \ldots \cup a_n} = \bar{a}_1 \cap \ldots \cap \bar{a}_n.$$

DEFINITION. (a) A set $Y \subseteq B$ is said to be a *family of sets with finite intersection property in the Boolean algebra* $\mathfrak{B}$ if the intersection in $\mathfrak{B}$ of any finite set of elements of Y is not 0. A family of sets with finite intersection property in $\langle P(X), \cup, \cap, {}^- \rangle$ (i. e. a set $Y \subseteq P(X)$ in which any finite subset has a nonempty intersection) will be called simply a *family of sets wlth finite intersection property*.

(b) A filter of the Boolean algebra $\mathfrak{B}$ contained in no filter of the algebra $\mathfrak{B}$ other than itself is called an *ultrafilter*.

It is clear that any filter of the Boolean algebra $\mathfrak{B}$ is a family of sets with finite intersection property in $\mathfrak{B}$.

PROPOSITION 1. *Every family Y of sets with finite intersection property in the Boolean algebra $\mathfrak{B}$ is contained in some ultrafilter of the algebra $\mathfrak{B}$.*

PROOF. Consider a set $U = \{X \mid X$ is a family of sets with finite intersection property in $\mathfrak{B}$ and $Y \subseteq X\}$. Since $Y \in U$, we have $U \neq \varnothing$. It is obvious that in the poset $\langle U, \subseteq \rangle$ the union of any chain is an element of U. By Theorem 1 there is a maximal element X_0 in $\langle U, \subseteq \rangle$. It suffices to show that X_0 is a filter. Condition (1) holds trivially for X_0. By virtue of the maximality of X_0, to verify conditions (2) and (3) it suffices to show that if $a, b \in X_0$ and $a \leqslant c$, then $X_0 \cup \{a \cap b\}$ and $X_0 \cup \{c\}$ are families of sets with finite intersection property in $\mathfrak{B}$. That $X_0 \cup \{a \cap b\}$ is a family of sets with finite intersection property is obvious. Suppose that $a_1 \cap \ldots \cap a_n \cap c = 0$ for some $a_1, \ldots, a_n \in X_0$. Then the equation $c \cap a = a$ yields

$$0 = 0 \cap a = (a_1 \cap \ldots \cap a_n \cap c) \cap a = (a_1 \cap \ldots \cap a_n) \cap \\ \cap (c \cap a) = a_1 \cap \ldots \cap a_n \cap a,$$

which contradicts the fact that X_0 is a family of sets with finite intersection property. □

PROPOSITION 2. *For a filter D of the Boolean algebra $\mathfrak{B}$ to be an ultrafilter it is necessary and sufficient that for any $b \in B$ either $b \in$ $\in D$ or $\bar{b} \in D$.*

PROOF. By virtue of Proposition 1, to prove necessity we must show that for any $b \in B$ either $D \cup \{b\}$ or $D \cup \{\bar{b}\}$ is a family of sets with finite intersection property in $\mathfrak{B}$. Suppose that this is not the case. Then $b_1 \cap \ldots \cap b_n \cap b = 0$ and $b_{n+1} \cap \ldots \cap b_{n+m} \cap$ $\cap \bar{b} = 0$ for some $b_1, \ldots, b_{n+m} \in D$. By property (2) of a filter D it may be assumed that $n = m = 1$. From the properties of the operations $\cup$, $\cap$, $^-$ in the Boolean algebra $\mathfrak{B}$ we get

$$b_1 \cap b_2 = b_1 \cap b_2 \cap (b \cup \bar{b}) = (b_1 \cap b_2 \cap b) \cup (b_1 \cap b_2 \cap \bar{b}) = \\ = (0 \cap b_2) \cup (b_1 \cap 0) = 0 \cup 0 = 0,$$

which contradicts properties (1), (2) of a filter D.

Sufficiency. If there is a filter $D^* \supseteq D$ and an element $b \in D^* \setminus D$, then $\bar{b} \notin D$ since otherwise $0 = b \cap \bar{b} \in D^*$, which is impossible. □

DEFINITION. A filter D of the Boolean algebra $\mathfrak{B}$ is said to be *principal* if there is $a_0 \in D$ such that

$$D = \{b \in B \mid a_0 \leqslant b\}.$$

An element $a \in B$ is said to be an *atom of the Boolean algebra* $\mathfrak{B}$ if $a \neq 0$ and

$$b \leqslant a \Rightarrow (b = a \quad \text{or} \quad b = 0).$$

It is clear that if a is an atom of $\mathfrak{B}$, then $b \cap a$ is equal to a or 0 for any $b \in B$.

LEMMA 2. *If D is a principal ultrafilter of the algebra $\mathfrak{B}$, then $D = \{b \in B \mid a_0 \leqslant b\}$ for some atom a_0* of $\mathfrak{B}$.

PROOF. Let $D = \{b \in B \mid b_0 \leqslant b\}$ for some $b_0 \neq 0$. Suppose that b_0 is not an atom. Then there is $b_1 \leqslant b_0$, $b_1 \neq b_0$, $b_1 \neq 0$. Since $b_1 \notin D$, by Proposition 2 $\bar{b}_1 \in D$, whence $b_0 \leqslant \bar{b}_1$, i. e. $b_0 \cap \bar{b}_1 = b_0$. Hence

$$b_1 = b_1 \cap b_0 = b_1 \cap (b_0 \cap \bar{b}_1) = b_0 \cap (b_1 \cap \bar{b}_1) = 0,$$

a contradiction. □

PROPOSITION 3. *The following conditions for the Boolean algebra $\mathfrak{B}$ are equivalent:*

(1) *B is a finite set;*

(2) *all nonempty filters of $\mathfrak{B}$ are principal;*

(3) *all ultrafilters of $\mathfrak{B}$ are principal.*

PROOF. (1) $\Rightarrow$ (2). If B is a finite set and $D = \{b_1, \ldots, b_n\}$ are filters of $\mathfrak{B}$, then the intersection $a_0 = b_1 \cap \ldots \cap b_n$ is in D and $a_0 \leqslant b_i$ for $i = 1, \ldots, n$. The statement (2) $\Rightarrow$ (3) is trivial. We prove (3) $\Rightarrow$ (1). Let (3) hold. Let $A_0 \subseteq B$ be the set of all atoms of $\mathfrak{B}$. Consider a set $A_1 = \{\bar{a} \mid a \in A_0\}$. We show that A_1 is not a family of sets with finite intersection property. Indeed, if A_1 is a family of sets with finite intersection property, by Proposition 1 $A_1 \subseteq D$ for some ultrafilter D. From condition (3) and Lemma 2 it follows that there is $a_0 \in A_0$ such that $a_0 \leqslant b$ for all $b \in D$. In particular, $a_0 \leqslant \bar{a}_0$, i. e. $a_0 = a_0 \cap \bar{a}_0 = 0$, which contradicts the condition $a_0 \neq 0$ for atoms $a \in A_0$. Since A_1 is not a family of sets with finite intersection property, $a_1 \cap \dots \cap \bar{a}_n = 0$ for some $a_1, \dots, a_n \in A_0$. From Lemma 1 we then get

$$1 = \bar{0} = \overline{\bar{a}_1 \cap \dots \cap \bar{a}_n} = \bar{\bar{a}}_1 \cup \dots \cup \bar{\bar{a}}_n = a_1 \cup \dots \cup a_n.$$

Let b be an arbitrary element of B. Then

$$b = b \cap 1 = b \cap (a_1 \cup \dots \cup a_n) = \\ = (b \cap a_1) \cup \dots \cup (b \cap a_n).$$

Since $b \cap a_i$ is equal to a_i or 0, b is equal to 0 or to the union of some elements of the set $\{a_1, \dots, a_n\}$. Hence B is a finite set. ☐

PROPOSITION 4. *If D is a principal ultrafilter on a set I, then $D = \{X \subseteq I \mid i_0 \in X\}$ for some $i_0 \in I$.*

PROOF. Follows from Lemma 2 since it is obvious that one-element sets are the atoms in $P(I)$. ☐

Exercises

1. Let D be a nonempty filter of the Boolean algebra $\mathfrak{B} = \langle B, \cup, \cap, ^- \rangle$. We define on the set B a relation $\tilde{D}$ as follows:

$$a \tilde{D} b \Leftrightarrow (a \cap \bar{b}) \cup (b \cap \bar{a}) \in \bar{D},$$

where $\bar{D}$ is equal to $\{\bar{d} \mid d \in D\}$. Show that $\tilde{D}$ is an equivalence on B and D is an ultrafilter if and only if B is divided by the relation $\tilde{D}$ into two equivalence classes.

2. A filter D on the set I is said to be countably complete if for any $a_i \in D$, $i \in \omega$, the set $\bigcap_{i \in \omega} a_i$ is in D. It is clear that any principal filter D on I is countably complete. Show that there is no nonprincipal countably complete ultrafilter on the set ω.

3. Let $\tilde{D}$ be an equivalence relation on B of Exercise 1. Let $B(D) = \{\tilde{D}_b \mid b \in B\}$ (the set $\tilde{D}_b$ is defined in Sec. 10 and is equal to $\{a \mid a \tilde{D} b, a \in B\}$). We define on $B(D)$ the operations $\cup$, $\cap$, $^-$ as follows:

(a) $m_1 \cup m_2 = \tilde{D}_{(a_1 \cup a_2)}$,
(b) $m_1 \cap m_2 = \tilde{D}_{(a_1 \cap a_2)}$,
(c) $\bar{m}_1 = \tilde{D}_{\bar{a}_1}$,

where $a_i \in m_i$, $i = 1, 2$. Show that such a definition is independent of the choice of elements $a_i \in m_i$ and $\langle B(D), \cup, \cap, ^- \rangle$ is a Boolean algebra.

13. THE POWER OF A SET

For infinite sets the notion of power may serve as a generalization of the concept of the number of elements.

DEFINITION. We shall say that the *power of a set A is less than or equal to the power of a set B* (and write $|A| \leqslant |B|$) if there is a distinct-valued mapping $f: A \to B$. We say that the *powers of the sets* A and B *are equal* or that A and B *are equipotent* (and write $|A| = |B|$) if there is a distinct-valued mapping of A onto B.

Notice that we have not as yet defined what the power of a set A is and have only defined two two-place relations on sets. It is these relations that are the basic notions of this section, the concept of power introduced below appearing merely for convenience of presentation.

Note the properties of the introduced relations that are immediate from the definition:

(a) $|A| \leqslant |A|$;

(b) $(|A| \leqslant |B|$ and $|B| \leqslant |C|) \Rightarrow |A| \leqslant |C|$;

(c) $|A| = |B| \Rightarrow (|A| \leqslant |B|$ and $|B| \leqslant |A|)$.

The following theorem shows that in property (c) $\Rightarrow$ may be replaced by $\Leftrightarrow$.

THEOREM 4. (Cantor-Bernstein). *If for sets A and B we have $|A| \leqslant |B|$ and $|B| \leqslant |A|$, then $|A| = |B|$.*

PROOF. Let $f: A \to B$, $g: B \to A$ be a distinct-valued mappings, $A_0 = A$, $A_1 = g[B]$ and $A_{n+2} = (fg)[A_n]$. By induction on n it is easily established that $A_{n+1} \subseteq A_n$, $n \in \omega$. Let $D = \bigcap_{k \in \omega} A_k$ and $M_i = A_i \setminus A_{i+1}$. It is obvious that $\left(\bigcup_{k \leqslant i \in \omega} M_i\right) \cup D = A_k$ and $M_i \cap M_j = \varnothing$ for $i \neq j$. Since $f \cdot g$ maps in a distinct-valued manner M_i onto M_{i+2} for any $i \in \omega$, a mapping $h: A \to A$ defined as follows:

$$ha = \begin{cases} a, \text{ if } a \in \left(\bigcup\limits_{i \in \omega} M_{2i+1}\right) \cup D \\ (fg)(a) \text{ if } a \in \bigcup\limits_{i \in \omega} M_{2i} \end{cases}$$

is a distinct-valued mapping of A onto

$$\left(\bigcup_{1 \leqslant i \in \omega} M_i\right) \cup D = A_1.$$

Since $|B| = |A_1|$, we get $|B| = |A|$. □

THEOREM 5 (Cantor). *The condition $|P(A)| \leqslant |A|$ does not hold for any set A.*

PROOF. Suppose that there is a distinct-valued mapping $f\colon P(A) \to A$. Consider a set $X = \{a \in f[P(A)] \mid a \notin f^{-1}(a)\}$. If $f(X) \in X$, then from the definition of X we get $f(X) \notin \notin f^{-1}(f(X)) = X$. If $f(X) \notin X$, then $f(X) \notin f^{-1}(f(X))$, hence $f(X) \in X$. The obtained contradiction shows that there can be no such f. □

THEOREM 6. *For any sets A and B either $|A| \leqslant |B|$ or $|B| \leqslant \leqslant |A|$.*

PROOF. By Theorem 2 there are $U \subseteq A^2$ and $V \subseteq B^2$ such that $\mathfrak{A} = \langle A, U\rangle$ and $\mathfrak{B} = \langle B, V\rangle$ are well-ordered sets. The statement of this theorem now follows from Theorem 3. □

For a set X we define a two-place relation $\varepsilon(X)$ consisting of pairs $\langle a, b\rangle \in X^2$ such that $a \in b$ or $a = b$. The set X is said to be *transitive* if $b \in X$ implies $b \subseteq X$.

DEFINITION. A set α is said to be an *ordinal* if it is transitive and $\langle \alpha, \varepsilon(\alpha)\rangle$ is a well-ordered set.

PROPOSITION 1. *The elements of an ordinal α are ordinals.*

PROOF. Since $\beta \subseteq \alpha$ for any $\beta \in \alpha$ the relation $\varepsilon(\beta) = \varepsilon(\alpha) \cap \beta^2$ is a well-founded linear ordering on $\beta \in \alpha$. If the element β of the ordinal α were not transitive, then for some γ_1 and γ_2 we should have $\gamma_1 \in \gamma_2 \in \beta$ and $\gamma_1 \notin \beta$. Since α is transitive, $\gamma_1, \gamma_2 \in \alpha$. This contradicts the transitivity of the relation $\varepsilon(\alpha)$. □

It is obvious that the natural numbers

$$\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \ldots$$

(each succeeding number containing all the preceding ones) are ordinals. The set ω of all natural numbers is also an ordinal. Ordinals are the sets $\omega \cup \{\omega\}$, $\omega \cup \{\omega\} \cup \{\omega, \{\omega\}\}$ and so on. In general, if α is an ordinal, then it is clear that the set $\alpha \cup \{\alpha\}$ is also an ordinal, which by analogy with the natural numbers is sometimes denoted by $\alpha + 1$.

PROPOSITION 2. *If α_1, α_2 are two distinct ordinals, then either $\alpha_1 \in \alpha_2$ or $\alpha_2 \in \alpha_1$.*

PROOF. We first show that either $\alpha_1 \subseteq \alpha_2$ or $\alpha_2 \subseteq \alpha_1$. If this is not the case, then by virtue of the transitivity of α_1, α_2 and the well ordering of $\langle \alpha_1, \varepsilon(\alpha_1)\rangle$, $\langle \alpha_2, \varepsilon(\alpha_2)\rangle$ there are $\gamma_1 \in \alpha_1$, $\gamma_2 \in \alpha_2$ such that $\gamma_1 \subseteq \gamma_2$, $\gamma_2 \subseteq \alpha_1$, $\gamma_1 \notin \alpha_2$, $\gamma_2 \notin \alpha_1$. Let $\delta \in \gamma_1$. Then $\delta \in \alpha_2$, and if $\delta \notin \gamma_2$, then by the linear ordering of $\langle \alpha_2, \varepsilon(\alpha_2)\rangle$ either $\delta =$

$= \gamma_2$ or $\gamma_2 \in \delta$. In both cases the transitivity of α_1 yields $\gamma_2 \in \alpha_1$, which is impossible. Thus $\gamma_1 \subseteq \gamma_2$. Similarly, it is shown that $\gamma_2 \subseteq \gamma_1$, hence by the axiom of extensionality $\gamma_1 = \gamma_2$, which contradicts the conditions $\gamma_1 \in \alpha_1$ and $\gamma_2 \notin \alpha_1$.

So it is shown that $\alpha_1 \subseteq \alpha_2$ or $\alpha_2 \subseteq \alpha_1$. Let $\alpha_2 \subseteq \alpha_1$, for example. Since $\alpha_1 \neq \alpha_2$, by the well ordering of $\langle \alpha_1, \varepsilon(\alpha_1)\rangle$ there is $\beta \in \alpha_1$ such that $\beta \subseteq \alpha_2$ and $\beta \neq \alpha_2$. Let $\delta \in \alpha_2$, then $\delta \in \alpha_1$ and $\delta \subseteq \alpha_2$. By the well ordering of $\langle \alpha_1, \varepsilon(\alpha_1)\rangle$ we have one of the following conditions: $\beta \in \delta$, $\beta = \delta$ or $\delta \in \beta$. The first two are impossible by the transitivity of α_2 and $\beta \neq \alpha_2$. Thus $\alpha_2 \subseteq \beta$, which together with $\beta \subseteq \alpha_2$ yields $\alpha_2 = \beta \in \alpha_1$. □

For a set X we define a set

$$\bigcup X = \{a \mid a \in x \quad \text{for some} \quad x \in X\}$$

called the *union* or *sum* of the set X.

An ordinal other than zero and not of the form $\alpha + 1$ is called a *limit ordinal*. It is clear that ordinal $\delta \neq 0$ is a limit ordinal if and only if $\bigcup \delta = \delta$. The set of the natural numbers ω may be defined to be such an ordinal all of whose elements are not limit elements.

PROPOSITION 3. *If X is a set of ordinals, then $\bigcup X$ is an ordinal.*

PROOF. The transitivity of $\bigcup X$ follows from the transitivity of the elements of X. The linear ordering of $\langle \bigcup X, \varepsilon(\bigcup X)\rangle$ follows from Proposition 2. If $Y \subseteq \bigcup X$, $\langle Y, \varepsilon(Y)\rangle$ has no minimal element and Y is not empty, then for any $a \in Y$ the set a is not empty and $\langle a \cap Y, \varepsilon(a \cap Y)\rangle$ has no minimal element. Since by Proposition 1 a is an ordinal, this is impossible, hence $\langle \bigcup X, \varepsilon(\bigcup X)\rangle$ is a well-ordered set.

PROPOSITION 4. *If X is a set of ordinals, then $\langle X, \varepsilon(X)\rangle$ is a well-ordered set.*

PROOF. If $a \in X$, then by Proposition 2 either $a \in b$ for some $b \in X$ or $a = \bigcup X$. Hence $X \subseteq ((\bigcup X) + 1)$ and the statement follows from Proposition 3. □

PROPOSITION 5. *For any well-ordered set $\mathfrak{A} = \langle A, U\rangle$ there is a unique ordinal $\alpha(\mathfrak{A})$ such that $\langle \alpha(\mathfrak{A}), \varepsilon(\alpha(\mathfrak{A}))\rangle$ is similar to $\mathfrak{A}$. We call this ordinal a type of a well-ordered set $\mathfrak{A}$.*

PROOF. Uniqueness follows from Proposition 11.5, since by Proposition 2 one of any two distinct ordinals α, β is the initial segment of the other.

Consider the set $X \subseteq A$ of all $a \in A$ such that there is an ordinal $\alpha(a)$ and a similarity f_a of a well-ordered set $\langle \alpha(a), \varepsilon(\alpha(a))\rangle$ onto $\langle O[a], U \cap (O[a])^2\rangle$, where $O[a] = O[a, \mathfrak{A}]$. By Proposition 11.5 the similarity f_a is uniquely defined by $a \in X$. Let $c \in X$ and $\langle b, c\rangle \in U$. It is obvious that $\alpha_0 = \{f_c^{-1}a \mid a \in O[b]\}$ is an ordinal. Since $f_c \restriction \alpha_0$ is a similarity of $\langle \alpha_0, \varepsilon(\alpha_0)\rangle$ onto $\langle O[b], U \cap \cap (O[b])^2\rangle$, we have $b \in X$ and $f_b = f_c \restriction \alpha_0$, hence $f_b \subseteq f_c$. Thus the mapping $f_0 = \bigcup \{f_a \restriction a \in X\}$ is a similarity of $\langle \beta_0, \varepsilon(\beta_0)\}$ onto $\langle X, U \cap X^2\rangle$, where β_0 is an ordinal equal to $\bigcup \{\alpha(a) \mid a \in X\}$. If $X = A$, then everything is proved. Suppose that $X \neq A$. Since X is the initial segment of $\mathfrak{A}$ and since $\mathfrak{A}$ is a well-ordered set, there is $a_0 \in A$ such that $X = O(a_0)$. It is obvious that $f_0 \cup \{\langle \beta_0, a_0\rangle\}$ is a similarity of the ordinal $\beta_0 \cup \{\beta_0\}$ onto $X \cup \{a_0\} = O[a_0]$, therefore $a_0 \in X$, which contradicts the choice of a_0. ☐

We shall say that the ordinal β is less than the ordinal α (and write $\beta < \alpha$) if $\beta \in \alpha$. If $\beta < \alpha$ or $\beta = \alpha$, we shall write $\beta \leqslant \alpha$. By Proposition 4 any set of ordinals is well-ordered by the relation $\leqslant$. If $\alpha_1, \ldots, \alpha_n$ are ordinals, then the element of the set $\{\alpha_1, \ldots \ldots, \alpha_n\}$ which is the greatest in the relation $\leqslant$ will be denoted by $\max \{\alpha_1, \ldots, \alpha_n\}$.

DEFINITION. An ordinal $\varkappa$ is said to be a *cardinal* if it is not equivalent to any smaller ordinal.

PROPOSITION 6. *The natural numbers* $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, ... *and the set* ω *of all natural numbers are cardinals.*

PROOF. To show that all natural numbers are cardinals it suffices to show by induction on $n \in \omega$ that no natural number n is equivalent to any of its subsets $w \neq n$. For $n = 0$ this holds since $\varnothing$ has no subsets other than $\varnothing$. Let $f\colon n + 1 \to n + 1$ be a distinct-valued mapping and $\operatorname{rang} f \neq n + 1$. If $n \notin \operatorname{rang} f$ or $f(n) = n$, then $f \restriction n$ maps n onto a subset $w \subseteq n$, $w \neq n$, which is impossible by the induction hypothesis. (Recall that $n + 1 = = \{0, 1, \ldots, n\}$.) If $f(k) = n$, $k < n$, then we define a mapping $g\colon n \to n$ for which $g(i) = f(i)$ for $i < n$, $i \neq k$, and $g(k) = f(n)$. Since $\operatorname{rang} g = \operatorname{rang} f \setminus \{n\}$ and $n \neq \operatorname{rang} f \setminus \{n\}$, g maps n onto $w \subseteq n$, $w \neq n$, which again contradicts the induction hypothesis. If ω were not a cardinal, then $|\omega| \leqslant n$ for some natural number n. We should then have $|n + 1| \leqslant |\omega| \leqslant |n|$, i. e. $n + 1$ is not a cardinal, which contradicts the foregoing. □

The following theorem makes it possible to select among equipotent sets a canonical representative, the cardinal.

THEOREM 7. *For any set X there is a unique cardinal $|X|$ equipotent to X.*

PROOF. The uniqueness of $|X|$ follows from the definition of a cardinal and Proposition 5.

By Theorem 2 there is $U \subseteq X^2$ such that $\langle X, U\rangle$ is a well-ordered set. By Proposition 5 there is an ordinal α_0 equipotent to X. As $|X|$ we take an ordinal $\beta \leqslant \alpha_0$, equipotent to α_0, all of whose elements are not equipotent to α_0. Such a cardinal exists by the well ordering of $\langle \alpha_0, \varepsilon(\alpha_0)\rangle$. □

DEFINITION. For a set X the cardinal $|X|$ of Theorem 7 is called the *power of the set X*.

It is obvious that $|\alpha| \leqslant \alpha$ for an ordinal α and that α is a cardinal if and only if $|\alpha| = \alpha$. Notice that the relation $|X| \leqslant |Y|$ on sets X and Y, defined at the beginning of this section, corresponds to the relation $\leqslant$ on the cardinals $|X|$ and $|Y|$ introduced above as follows: $\varkappa_1 \leqslant \varkappa_2 \Leftrightarrow (\varkappa_1 \in \varkappa_2$ or $\varkappa_1 = \varkappa_2)$. Now we give a precise definition of the property of being a finite set which we previously used intuitively.

DEFINITION. A set X is said to be *finite* if $|X| \in \omega$ and *countable* (denumerable or enumerable) if $|X| = \omega$.

If X is not a finite set, then we say that X is infinite. Notice that there are infinite nonenumerable sets; moreover, by Theorem 5 the power of any set X is less than the power of a set $P(X)$. Since ω is the least infinite cardinal, countable sets have the least power among the infinite sets. It is obvious that a finite or countable set X can be represented as $X = \{a_n | n \in \omega\}$, the sequence

$$a_0, a_1, \ldots, a_n, \ldots, n \in \omega$$

being called the *numbering of the set X*. It is clear that if $Y \subseteq X$, then $|Y| \leqslant |X|$. Notice that the infinite cardinal $\varkappa$ cannot be of the form $\alpha + 1 = \alpha \cup \{\alpha\}$. Indeed, since α is an infinite ordinal, by Proposition 2 $\omega \subseteq \alpha$, therefore the mapping $f: \alpha + 1 \twoheadrightarrow \alpha$ for which

$$f(\beta) = \begin{cases} \beta & \text{if } \beta \notin \omega \cup \{\alpha\} \\ \varnothing & \text{if } \beta = \omega \\ \beta + 1 & \text{if } \beta \in \omega \end{cases}$$

is distinct-valued, hence $|\alpha + 1| = |\alpha| \leqslant \alpha$. We prove the following important theorem.

THEOREM 8. *If a set A is infinite, then $|A| = |A^2|$.*

PROOF. A mapping $f\colon A \to A^2$ for which $f(a) = \langle a, a\rangle$ is distinct-valued, hence $|A| \leqslant |A^2|$. Suppose that $|A^2| \leqslant |A|$ does not hold. Then the set $X = \{\alpha \mid \alpha$ is an infinite cardinal, $\alpha \leqslant |A|$ and $\alpha < |\alpha^2|\}$ is not empty and let α_0 be the least element of X. We define on the set α_0^2 the relation $\preccurlyeq$ as follows:

$$\langle \beta_1, \beta_2\rangle \preccurlyeq \langle \gamma_1, \gamma_2\rangle \Leftrightarrow \begin{cases} \max\{\beta_1, \beta_2\} < \max\{\gamma_1, \gamma_2\} & \text{or} \\ \max\{\beta_1, \beta_2\} = \max\{\gamma_1, \gamma_2\}, \beta_1 < \gamma_1, & \text{or} \\ \max\{\beta_1, \beta_2\} = \max\{\gamma_1, \gamma_2\}, \beta_1 = \gamma_1, \beta_2 \leqslant \gamma_2. \end{cases}$$

It is obvious that $\preccurlyeq$ is a linear ordering on α_0^2. Besides $\langle \alpha_0^2, \preccurlyeq\rangle$ is a well-ordered set, since for any nonempty subset $Y \subseteq \alpha_0^2$ there are nonempty subsets

$$Y_1 = \{\langle \beta, \gamma\rangle \in Y \mid \max\{\beta, \gamma\} \leqslant \max\{\beta', \gamma'\} \text{ for any } \langle \beta', \gamma'\rangle \in Y\},$$

$$Y_2 = \{\langle \beta, \gamma\rangle \in Y_1 \mid \beta \leqslant \beta' \text{ for any } \langle \beta', \gamma'\rangle \in Y_1\}$$

$$Y_3 = \{\langle \beta, \gamma\rangle \in Y_2 \mid \gamma \leqslant \gamma' \text{ for any } \langle \beta', \gamma'\rangle \in Y_2\}$$

and it is obvious that Y_3 contains exactly one element and that element is the least element of Y in the relation $\preccurlyeq$. Since $\alpha_0 < |\alpha_0^2|$, by Theorem 3 $\langle \alpha_0, \varepsilon(\alpha_0)\rangle$ is similar to the initial segment $Z = O(\langle \beta_0, \gamma_0\rangle)$ of a well-ordered set $\langle \alpha_0^2, \preccurlyeq\rangle$.

Let $\delta_0 = \max\{\beta_0, \gamma_0\}$. Then it is obvious that $Z \subseteq (\delta_0 + 1)^2$. Since α_0 is infinite, Z and δ_0 are also infinite and $|\delta_0 + 1| = \delta_0| < \alpha_0$. Then by the choice of cardinal α_0 we have

$$\alpha_0 = |Z| \leqslant |(\delta_0 + 1)^2| \leqslant |\delta_0 + 1| < \alpha_0,$$

a contradiction. □

COROLLARY 1. *Let A, B be sets and let at least one of them be infinite. Then*

(a) *if $A \neq \varnothing$ and $B \neq \varnothing$, then* $|A \times B| = \max\{|A|, |B|\}$;

(b) $|A \cup B| = \max\{|A|, |B|\}$.

PROOF. Let $|A| = \max\{|A|, |B|\}$.

(a) Let $b_0 \in B$. Then a mapping $f: A \to A \times B$ for which $f(a) = \langle a, b_0 \rangle$ is distinct-valued, therefore $|A| \leqslant |A \times B|$. From $|B| \leqslant |A|$ and the preceding theorem we get

$$|A \times B| \leqslant |A^2| = |A|.$$

(b) It is obvious that $|A| \leqslant |A \cup B|$. Let $f: B \to A$ be a distinct-valued mapping. Then a mapping $g: A \cup B \to A \times \{0, 1\}$ for which

$$g(a) = \begin{cases} \langle a, 0 \rangle & \text{if} \quad a \in A, \\ \langle fa, 1 \rangle & \text{if} \quad a \in B \setminus A \end{cases}$$

is distinct-valued, therefore from statement (a) we get

$$|A \cup B| \leqslant |A \times \{0, 1\}| = |A|. \square$$

COROLLARY 2. (a) *If A is infinite, then $|A^k| = |A|$ for any natural $k > 0$.*

(b) *If A is infinite and $A^* = \bigcup\{A^k \mid k \in \omega\}$, then $|A^*| = |A|$.*

(c) *If W is a set of words of an alphabet $A \neq \varnothing$, then* $|W| = \max\{|A|, \omega\}$.

PROOF (a) follows from Corollary 1(a) by induction on k.

(b) Let $f_k: A^k \to A$, $0 < k < \omega$, be distinct-valued mappings existing by virtue of statement (a). Then a mapping $f: A^* \to \omega \times A$ for which

$$fa = \begin{cases} \langle 0, a \rangle & \text{if} \quad a = \varnothing \in A^0 \\ \langle k, f_k a \rangle & \text{if} \quad a \in A^k \setminus (A^0 \cup \ldots \cup A^{k-1}), \quad k > 0 \end{cases}$$

is distinct-valued, by Corollary 1(a) therefore we get $|A^*| \leqslant |\omega \times A| = |A|$. The inverse inequality $|A| \leqslant |A^*|$ is obvious.

(c) Since for $a \in A$ the words a, aa, aaa, ... are pairwise distinct, $\omega \leqslant |W|$. If A is infinite, then statement (c) follows from statement (b). If $|A| = n \in \omega$, then obviously $|W| \leqslant |\omega^*|$ and again from (b) we get $|W| \leqslant \omega$. □

Exercises

1. Show that the sets of integers, rationals and algebraic numbers are countable.

2. Show that the sets of reals and complex numbers are equipotent and that the sets of reals and natural numbers are not equivalent. (*Hint*. Notice that the power of the set of reals is $|P(\omega)|$ and use Cantor's theorem.)

14. THE AXIOM OF CHOICE

Let us define the sets V_α, where α is an ordinal, as follows:

(a) $V_0 = \varnothing$;

(b) $V_\alpha = P(V_\beta)$ if $\alpha = \beta + 1$;

(c) $V_\alpha = \bigcup\limits_{\beta < \alpha} V_\beta$ if α is a limit ordinal.

The axiom stating that for any set X there is an ordinal α for which $X \in V_\alpha$ is called the *axiom of regularity*. Thus by the axiom of regularity every set is obtained at some step of a "regular process" in which, starting from an empty set, at each step all sets are obtained whose elements have already been obtained at the previous steps. This fully agrees with our intuitive ideas of how sets are formed.

The axiom of regularity allows every set X to be assigned an ordinal $\rho(X)$ which is called the *rank* of X and defined as the least ordinal for which $X \in V_{\rho(X)}$. It is obvious that if $X \in Y$, then $\rho(X) < \rho(Y)$, by virtue of Proposition 13.4 the axiom of regularity yields the following two statements:

(1) there is no sequence $X_0, X_1, \ldots, X_n, \ldots$ for which $X_{n+1} \in \in X_n$, $n \in \omega$;

(2) any set X has an element $a \in X$ for which $a \cap X = \varnothing$.

The axiom of regularity is in fact equivalent to each of the statements (1) and (2). Indeed, if $X_{n+1} \in X_n$ for $n \in \omega$, then the set $\{X_n \mid n \in \omega\}$ contradicts condition (2), hence (2) $\Rightarrow$ (1). Notice that if for any element a of a set X there is an ordinal $\beta(a)$ such that $a \in V_{\beta(a)}$, then $X \in V_\gamma$, where $\gamma = (\bigcup \{\beta(a) | a \in X\} + 1)$. Therefore if a_0 is in V_α for no ordinal α, then $a_1 \in a_0$ which is in V_α for no α either. Thus if the regularity axiom fails to hold, then there is a sequence $a_n, n \in \omega$ such that $a_{n+1} \in a_n$, $n \in \omega$, i. e. (1) also fails.

The axioms of extensionality and regularity impose certain conditions on the relation of $\in$ (membership) and that of $=$ (equality), i. e. in a sense they restrict the "Universe" consisting of sets. The axiom of choice, on the contrary, states that there must be certain sets in this "Universe" if there are already some. In our proofs, however, we freely used other conditions for the existence of sets as well, for example, we formed a union $A \cup B$ of two sets A and B, discussed a power set $P(A)$, assumed that natural numbers $n \in \omega$ "are available". All the conditions of the existence of sets we have used (except the axiom of choice) are obtained from the following axioms of "existence":

(1) There is an empty set $\varnothing$.

(2) If there are sets a and b, then there is a set $\{a, b\}$.

(3) If there is a set X, then there is a set $\bigcup X = \{t | t \in x$ for some element $x \in X\}$.

(4) There is a set $\omega = \{0, 1, \ldots, n, \ldots\}$, where $0 \neq \varnothing$ and $n + 1 = n \cup \{n\}$.

(5) If there is a set A, then there is a set $P(A) = \{B | B \subseteq A\}$.

(6) If $\Phi(x, y)$ is some condition on sets x, y such that for any set x there is at most one set y satisfying the condition $\Phi(x, y)$, then for any set a there is a set

$$\{b | \Phi(c, b) \text{ for some element } c \in a\}.$$

EXAMPLE 1. We show that axioms (5) and (6) imply the existence of a set $A^2 = \{\langle a, b\rangle | a, b \in A\}$ for any set A.

Since $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$, we have $A^2 \subseteq P(P(A))$. Let $\Phi_0(x, y) \Leftrightarrow$ (there are $a, b \in A$ such that

$$x = \{\{a\}, \{a, b\}\} \quad \text{and} \quad y = x).$$

Then the set A^2 is equal to $\{b | \Phi_0(c, b), c \in P(P(A))\}$ and by axiom (6) it exists.

The system of axioms (1) to (6) together with the axioms of extensionality and regularity is called the *Zermelo-Fraenkel axiom system* (abbreviated ZF). The system ZF together with the axiom of choice is denoted by ZFC *.

Within ZFC it is possible to develop all modes of reasoning generally accepted in mathematics today. One may even say that at the present stage of mathematical development this "translatability" into ZFC is a measure of mathematical rigour. (True, this is questioned by intuitionists and constructivists, but we are not concerned with their views in this book.) Thus a formal derivation from the axioms of ZFC may be taken as a reasonable refinement of the concept of mathematical proof**. A precise formulation of this notion is of great significance. It is one of the central problems of mathematical logic. Only with appropriate precise definitions at one's disposal can one establish the unprovability and independence of some statements. Thus it was proved that a set of real numbers can be assigned practically any power without contradiction. The fact that the validity of a formal proof can be easily verified by computer formed the starting point for long-range studies of machine proof search. Historically ZFC came into being mainly due to the discovery of inconsistencies in the "naive" theory of sets. What can be said about the consistency of ZFC? No inconsistencies have been discovered in ZFC itself thus far. On the other hand, it was proved that if ZFC is consistent, this cannot be established using its own means. So the proof of the consistency of ZFC appears to be somehow related to a revision of our usual ideas about a mathematical proof.

There are seven axioms in ZFC stating the existence of some sets. The axiom of choice occupies a particular place among them. It appears to be the least "obvious". The thing is that sets whose existence is asserted in axioms (1) to (6) are uniquely defined (for example, the sum of a set $\bigcup X$ is uniquely defined by X), but the function of choice for nonempty subsets of X is ambiguously defined. Moreover, if there is a condition that uniquely defines the function of choice for nonempty subsets of X, then the existence of a function of choice for $P(X) \setminus \{\varnothing\}$ can be derived without the axiom of choice (i. e. in ZF). The presence of an uncertainty of an object whose existence is asserted aroused numerous debates around the axiom of choice among mathematicians early in the twentieth century. Some even thought that it must surely lead to a contradiction. These debates on the whole subsided, however, after K. Gödel's result about the equiconsistency of ZF and ZFC. Nevertheless up to the present some try sometimes to give, if possible, proofs without the axiom of choice considering such a proof to be more "constructive".

---

* For a precise definition of the notion of condition $\Phi(x, y)$ in axiom (6) we refer the reader to the notion of formula of the signature Σ_0 containing only one two-place predicate sign $\in$ (see Chapter 3). Notice that all axioms for ZFC can be written as proposition of the signature Σ_0.

** By formal derivation we mean derivation in the calculus of predicates (see Sec. 22).

The remainder of this section is devoted to a theorem which shows that the axiom of choice is equivalent (in ZF) to some of its consequences proved in the preceding sections.

THEOREM 9. *From the axioms for* ZF *one can derive the equivalence of the following statements*:

(a) *the axiom of choice*: *for any nonempty set A there is a mapping h: $(P(A) \setminus \{\varnothing\}) \to A$ such that $hB \in B$ for all $B \subseteq A$, $B \neq \varnothing$*;

(b) *the principle of well ordering*: *for any set A there is a relation $U \subseteq A^2$ such that $\langle A, U\rangle$ is a well-ordered set*;

(c) *the maximum principle*: *if in a partially ordered set $\mathfrak{A} = \langle A, U\rangle$ each chain has an upper bound, then $\mathfrak{A}$ has a maximal element*;

(d) *if A is an infinite set, then $|A^2| = |A|$.*

PROOF. By Theorems 1, 2 and 8 we have in ZF (a) $\Rightarrow$ (c), (a) $\Rightarrow$ (b) and (a) $\Rightarrow$ (d); in addition it is shown in the proof of Theorem 2 that in ZF (c) $\Rightarrow$ (b). It suffices therefore to derive (b) $\Rightarrow$ (a) and (d) $\Rightarrow$ (b) from the axioms for ZF.

(b) $\Rightarrow$ (a). Let $\langle A, U\rangle$ be a well-ordered set. Take as $\Phi(x, y)$ the following condition: $\Phi(x, y) \Leftrightarrow (\langle x, U \cap x^2\rangle$ is a well-ordered set,

$$\begin{gathered} y \text{ is an ordered pair, } \pi_1^2 y = x \text{ and} \\ \pi_2^2 y \text{ is the least element of } \langle x, U \cap x^2\rangle). \end{gathered}$$

It is obvious that for any x there is at most one y for which $\Phi(x, y)$ holds. It follows from axiom (6) that there is a set

$$h = \{\langle B, a\rangle \mid \Phi(B, \langle B, a\rangle), B \in (P(A) \setminus \{\varnothing\})\}.$$

It is clear that h: $(P(A) \setminus \{\varnothing\}) \to A$ and $h(B) \in B$ for $B \subseteq A$, $B \neq \varnothing$.

(d) ⇒ (b). Since $\langle n, \varepsilon(n)\rangle$ is a well-ordered set for any $n \in \omega$, it suffices to treat the case where A is infinite. Axiom (6) implies the existence of a set

$$W = \{U \subseteq A^2 \mid \langle D(U), U\rangle \text{ is a well-ordered set}\},$$

where $D(U) = \{a \in A \mid \langle a, b\rangle \in U$ or $\langle b, a\rangle \in U$ for some $b \in A\}$. If $U \in W$, then by $\alpha(U)$ we denote the type of the set $\langle D(U), U\rangle$ (Proposition 13.5). By axiom (6) there is a set $V = \{\alpha(U) \mid U \in W\}$. It is clear that V is equal to the set $\{\alpha \mid \alpha$, an ordinal, and $|\alpha| \leqslant |A|\}$. By Proposition 13.3 $\alpha_0 = \bigcup V$ is an ordinal. If there is a distinct-valued mapping f: $\alpha_0 \to A$, then $\{f\beta \mid \beta \in \alpha_0\} = A$, since otherwise the mapping $f \cup \{\langle \alpha_0, a_0\rangle\}$, where $a_0 \in A \setminus \{f\beta \mid \beta \in \alpha_0\}$, will be a distinct-valued mapping of $\alpha_0 + 1$ into A, hence $\alpha_0 + 1 \subseteq \alpha_0$, which is impossible. Thus either $|\alpha_0| = |A|$ or $|\alpha_0| \leqslant |A|$ does not hold. If $|\alpha_0| = |A|$, then the well ordering of $\langle \alpha_0, \varepsilon(\alpha_0)\rangle$ yields the well ordering of $\langle A, U\rangle$ for some $U \subseteq A^2$. Let $|\alpha_0| \leqslant |A|$ fail to hold. By induction on $n \in \omega$ it is easy to get $|n| \leqslant |A|$ for any $n \in \omega$, hence α_0 is an infinite ordinal. Consider a set $X = \{\langle \alpha_0 a\rangle \mid a \in A\}$. It is obvious that $|X| = |A|$ and $X \cap \alpha_0 = \varnothing$. For simplicity we denote the equipotency $|E| = |F|$ by $E \sim F$.

Notice that if $|Y| \leqslant |Z|$ and Z is infinite, then $Y \cup Z \sim Z$. Indeed, if g: $Y \to Z$ is a distinct-valued mapping, $z_1, z_2 \in Z$, $z_1 \neq z_2$, then a mapping f: $Y \cup Z \to Z^2$ for which

$$fa = \begin{cases} \langle z_1, ga\rangle & \text{if} \quad a \in Y \\ \langle z_2, a\rangle & \text{if} \quad a \in Z \setminus Y \end{cases}$$

is distinct-valued, so $|Y \cup Z| \leqslant |Z^2|$. From (d) we have $|Z^2| = |Z|$, hence $|Y \cup Z| \leqslant |Z|$. The condition $|Z| \leqslant |Y \cup Z|$ is obvious. Using this fact and condition (d) we get

$$\alpha_0 \cup X \sim (\alpha_0 \cup X)^2 = \alpha_0^2 \cup (\alpha_0 \times X) \cup X^2 \cup (X \times \alpha_0) \sim$$
$$\sim \alpha_0 \cup (\alpha_0 \times X) \cup X \cup (X \times \alpha_0) \sim (\alpha_0 \times X) \cup (X \times \alpha_0) \sim \alpha_0 \times X.$$

Thus $\alpha_0 \times X = C \cup D$, where $C \sim \alpha_0$ and $D \sim X \sim A$. We show that $(\alpha_0 \times \{x\}) \cap C \neq \varnothing$ for any $x \in X$. Indeed, otherwise $(\alpha_0 \times \{x_0\}) \subseteq D$ for some $x_0 \in X$, hence $|\alpha_0 \times \{x_0\}| \leqslant |D|$. Since $\alpha_0 \sim (\alpha_0 \times \{x_0\})$ and $D \sim A$, this contradicts the fact that $|\alpha_0| \leqslant |A|$ fails to hold. Since $C \sim \alpha_0$ and $\langle \alpha_0, \varepsilon(\alpha_0)\rangle$ is a well-ordered set, there is $U \subseteq C^2$ for which $\langle C, U\rangle$ is a well-ordered set. Using axiom (6) it is easy to obtain a mapping $f: X \to C$ for which fa is equal to the element of $(\alpha_0 \times \{a\}) \cap C$ that is the least with respect to the relation U. It is obvious that f is a distinct-valued mapping. The statement (d) ⇒ (b) now follows from $A \sim X$ and the well ordering of $\langle f[X], U \cap (f[X])^2\rangle$. □

Exercise

1. Show that the axiom of choice is equivalent in ZF to the following statement, if M is a partition of a set A (see Example 1), then there is a mapping $g: M \to A$ for which $g(m) \in m$, $m \in M$, $m \neq \varnothing$. (*Hint*. Consider a partition $\{m(B) \mid B \in P(A) \setminus \{\varnothing\}\}$, where $m(B) = \{\langle B, a\rangle \mid a \in B\}$.)

Chapter 3

TRUTH ON ALGEBRAIC SYSTEMS

15. ALGEBRAIC SYSTEMS

Frequently the object of study in mathematics is a set together with a structure defined on it. For example: the set of triangles with similarity relation, the set of real numbers with the operations of addition and multiplication, the set of real functions with the property of differentiability and the operation of differentiation and so on. In this section we give a more precise definition of this concept by introducing a definition of an algebraic system.

DEFINITION. The ordered triple $\Sigma = \langle R, F, \mu \rangle$ is said to be a *signature* if the following conditions hold:

(a) the sets R and F have no elements in common;

(b) μ is a mapping of the set $R \cup F$ into ω.

Elements of the set R are called *relation* or *predicate symbols*. Elements of the set F are called *operation* or *function symbols*. The mapping μ is called a *place* or *arity mapping for* Σ. If $\mu(q) = n$, then q is said to be an n-place predicate symbol when $q \in R$ and an n-place function symbol when $q \in F$. The 0-place function symbol is called the symbol of a constant or simply a constant.

For convenience we shall often represent the finite or countable signature $\Sigma = \langle R, F, \mu \rangle$ as

$$\Sigma = \langle r_1^{\mu(r_1)}, \ldots, r_n^{\mu(r_n)}, \ldots; f_1^{\mu(f_1)}, \ldots, f_k^{\mu(f_k)}, \ldots; c_1, \ldots, c_m, \ldots \rangle,$$

where r_i, f_j are relation and function symbols which are not constants, c_k are constants of the signature Σ. In what follows all signatures will be denoted by the letter Σ (possibly with indices), the set of their relation symbols by R, the set of operation symbols by F, and the arity mapping by μ (with the corresponding indices). We shall say that a signature Σ is contained in a signature Σ_1 (and write $\Sigma \subseteq \Sigma_1$) if $R \subseteq R_1$, $F \subseteq F_1$ and $\mu \subseteq \mu_1$. If $X \subseteq R \cup F$, then the signature $\Sigma_1 = \langle R \cap X, F \cap X, \mu \restriction X \rangle$ is said to be a restriction of the signature Σ to the set X (and we write $\Sigma_1 = \Sigma \restriction X$).

The power of the set $R \cup F$ is called the power of the signature $\Sigma = \langle R, F, \mu \rangle$ and denoted by $|\Sigma|$. If $\Sigma_n \subseteq \Sigma_{n+1}$, $n \in \omega$, then by $\bigcup_{n \in \omega} \Sigma_n$ we denote the signature $\left\langle \bigcup_{n \in \omega} R_n, \bigcup_{n \in \omega} F_n, \bigcup_{n \in \omega} \mu_n \right\rangle$.

If $R \cup F \neq \varnothing$ and $F = \varnothing (R = \varnothing)$, then a signature Σ is said to be a *predicate* (*function*) signature. If $R \cup F \neq \varnothing$, then the signature Σ is said to be empty.

DEFINITION. An ordered pair $\mathfrak{A} = \langle A, \nu^{\mathfrak{A}} \rangle$ is said to be an *algebraic system of a signature* Σ if the following conditions hold:

(a) A is a nonempty set;

(b) $\nu^{\mathfrak{A}}$ is a mapping of a set $R \cup F$ into relations and operations on a set A;

(c) $r \in R \Rightarrow \nu^{\mathfrak{A}}(r)$ is a $\mu(r)$-place relation on A;

(d) $f \in F \Rightarrow \nu^{\mathfrak{A}}(f)$ is a $\mu(f)$-place operation on A. The set A is called the *carrier* of $\mathfrak{A}$, and $\nu^{\mathfrak{A}}$ is an *interpretation of the signature* Σ in A.

In what follows we shall often write simply $r^{\mathfrak{A}}$ or even r instead of $\nu^{\mathfrak{A}}(r)$ if it is clear what $\mathfrak{A}$ is meant. In what follows algebraic systems will be denoted by the Gothic letters $\mathfrak{A}$ and $\mathfrak{B}$ (possibly with indices) and their carriers by the corresponding Latin letters A and B (with the corresponding indices). *The power of an algebraic system* $\mathfrak{A}$ is the power of its carrier A. For brevity we shall often omit the word "algebraic" and call $\mathfrak{A}$ simply a system.

DEFINITION. A mapping $f: A \rightarrow B$ is said to be a *homomorphism* of an algebraic system $\mathfrak{A}$ of Σ into a system $\mathfrak{B}$ of the same signature Σ if the following conditions hold:

(a) if $q \in R$ and $\mu(q) = n$, then for all $a_1, \ldots, a_n \in A$ $\langle a_1, \ldots, a_n \rangle \in q^{\mathfrak{A}} \Rightarrow \langle fa_1, \ldots, fa_n \rangle \in q^{\mathfrak{B}}\mathfrak{B}$;

(b) If $q \in F$ and $\mu(q) = n$, then for all $a_1, \ldots, a_n \in A$ $f(q^{\mathfrak{A}}(a_1, \ldots, a_n)) = q^{\mathfrak{B}}(fa_1, \ldots, fa_n)$.

If f is a homomorphism of $\mathfrak{A}$ into $\mathfrak{B}$ and $f[A] = B$, then f is said to be a *homomorphism* of $\mathfrak{A}$ *onto* $\mathfrak{B}$ and $\mathfrak{B}$ is said to be a *homomorphic image* of $\mathfrak{A}$.

A distinct-valued homomorphism f of $\mathfrak{A}$ onto $\mathfrak{B}$ for which f^{-1} is also a homomorphism is called an *isomorphism of* $\mathfrak{A}$ *onto* $\mathfrak{B}$ and denoted by $f: \mathfrak{A} \simeq \mathfrak{B}$. If there is an isomorphism $f: \mathfrak{A} \simeq \mathfrak{B}$ then the systems $\mathfrak{A}$ and $\mathfrak{B}$ are said to be *isomorphic* and this is designated as: $\mathfrak{A} \simeq \mathfrak{B}$. An isomorphism f of a system $\mathfrak{A}$ onto $\mathfrak{A}$ is called an *automorphism of the system* $\mathfrak{A}$.

PROPOSITION 1. (a) *If* $f\colon \mathfrak{A} \simeq \mathfrak{B}$ *then* $f^{-1}\colon \mathfrak{B} \simeq \mathfrak{A}$.

(b) *If* $f\colon \mathfrak{A} \simeq \mathfrak{A}_1$ *and* $g\colon \mathfrak{A}_1 \simeq \mathfrak{A}_2$, *then* $(fg)\colon \mathfrak{A} \simeq \mathfrak{A}_2$.

(c) $\mathrm{id}_A\colon \mathfrak{A} \simeq \mathfrak{A}$.

PROOF. Follows immediate from the definition of an isomorphism. □

DEFINITION. A system $\mathfrak{A}$ is said to be a *subsystem* of a system $\mathfrak{B}$ (and we write $\mathfrak{A} \subseteq \mathfrak{B}$) if the following conditions hold:

(a) $\mathfrak{A}$ and $\mathfrak{B}$ have the same signature;

(b) $A \subseteq B$;

(c) the set A is closed under the operations $\nu^{\mathfrak{B}}(f), f \in F$;

(d) relations and operations $\nu^{\mathfrak{A}}(q), q \in R \cup F$, in $\mathfrak{A}$ are restrictions to A of the corresponding relations and operations $\nu^{\mathfrak{B}}(q)$, $q \in R \cup F$, in $\mathfrak{B}$.

If $A \neq B$, then $\mathfrak{A} \subseteq \mathfrak{B}$ is said to be a *proper* subsystem of $\mathfrak{B}$. If $\mathfrak{A} \subseteq \mathfrak{B}$, then $\mathfrak{B}$ is said to be a *supersystem* of $\mathfrak{A}$.

It follows from the definition of a subsystem that two subsystems $\mathfrak{A}_1$, $\mathfrak{A}_2$ of a system $\mathfrak{B}$ with the same carriers coincide. On the other hand, if a nonempty subset $B_1 \subseteq B$ is closed under the operations of the system $\mathfrak{B}$, then B_1 is the carrier of some subsystem $\mathfrak{B}_1 \subseteq \mathfrak{B}$. Thus there is a distinct-valued mapping of a set of nonempty subsets of B closed under the operations of $\mathfrak{B}$ onto a set of subsystems of $\mathfrak{B}$. That mapping can be extended to all nonempty subsets of B. Namely, we have

PROPOSITION 2. *If* $\mathfrak{B}$ *is an algebraic system*, $X \subseteq B$, $X \neq \varnothing$, *then there is a unique subsystem* $\mathfrak{B}(X) \subseteq \mathfrak{B}$ *with carrier* $B(X)$ *such that* $X \subseteq B(X)$ *and* $\mathfrak{B}(X) \subseteq \mathfrak{A}$ *for any subsystem* $\mathfrak{A} \subseteq \mathfrak{B}$ *for which* $X \subseteq A$.

PROOF. As $B(X)$ we take the intersection of the carriers A of all subsystems $\mathfrak{A} \subseteq \mathfrak{B}$ containing X. Since $X \subseteq B(X)$, we have $B(X) \neq \varnothing$. As already noted above, $B(X)$ is the carrier of a unique subsystem $\mathfrak{B}(X) \subseteq \mathfrak{B}$. □

DEFINITION. The subsystem $\mathfrak{B}(X) \subseteq \mathfrak{B}$ of Proposition 2 is called a *subsystem generated by a set* X *in* $\mathfrak{B}$. If $X = \{a_1, \ldots, a_n\}$, then $\mathfrak{B}(X)$ is also denoted by $\mathfrak{B}(a_1, \ldots, a_n)$. If $\mathfrak{B}(X) = \mathfrak{B}$, then we say that the system $\mathfrak{B}$ is generated by the set X.

A set of algebraic systems $\{\mathfrak{A}_i \mid i \in I\}$ is said to be a *directed set of algebraic systems* if $I \neq \varnothing$ and for any $i, j \in I$ there is $k \in I$ for which $\mathfrak{A} \subseteq \mathfrak{A}_k$ and $\mathfrak{A}_j \subseteq \mathfrak{A}_k$. It follows from the definition that all systems of a directed set of systems have the same signature.

PROPOSITION 3. *If* $\{\mathfrak{A}_i \mid i \in I\}$ *is a directed set of algebraic systems of* Σ, *then there is a unique system* $\mathfrak{A}$ *such that* $\mathfrak{A}_i \subseteq \mathfrak{A}$ *for all* $i \in I$ *and* $\mathfrak{A} \subseteq \mathfrak{B}$ *for any system* $\mathfrak{B}$ *for which* $\mathfrak{A}_i \subseteq \mathfrak{B}$, $i \in I$.

PROOF. The carrier of $\mathfrak{A}$ will be a set $A = \bigcup\limits_{i \in I} A_i$. Let $\{a_1, \ldots, a_n\} \subseteq A$. Then it follows from the definition of a directed set that there is $i \in I$ such that $\{a_1, \ldots, a_n\} \subseteq A_i$. Let $\langle a_1, \ldots, a_n \rangle$ belong to $\nu^{\mathfrak{A}}(s)$, $s \in R \cup F$ precisely if $\langle a_1, \ldots, a_n \rangle$ belongs to $\nu^{\mathfrak{A}_i}(s)$. Such a definition is independent of the choice of $i \in I$, since if $\{a_1, \ldots, a_n\} \subseteq A_j$, then there is $\mathfrak{A}_k$ such that $\mathfrak{A}_i \subseteq \mathfrak{A}_k$ and $\mathfrak{A}_j \subseteq \mathfrak{A}_k$. Hence $\nu^{\mathfrak{A}_\tau}(r) \cap \{\langle a_1, \ldots, a_n \rangle\}$, $r \in R$, and $\nu^{\mathfrak{A}_\tau}(f)(a_1, \ldots, a_n)$, $f \in F$, for $\tau \in \{i, j\}$ coincide with the corresponding $\nu^{\mathfrak{A}_k}(r) \cap \{\langle a_1, \ldots, a_n \rangle\}$, $r \in R$, and $\nu^{\mathfrak{A}_k}(f)(a_1, \ldots, a_n)$, $f \in F$. The second statement of the proposition and the uniqueness of $\mathfrak{A}$ are obvious. □

The system $\mathfrak{A}$ of Proposition 3 is called the *union of systems* $\mathfrak{A}_i$, $i \in I$ and designated $\mathfrak{A} = \bigcup\limits_{i \in I} \mathfrak{A}_i$.

DEFINITION. An algebraic system $\mathfrak{A}$ of Σ is said to be an *expansion* of a system $\mathfrak{A}_1$ of Σ_1 if the following conditions hold:

(a) $A = A_1$;

(b) $\Sigma_1 = \Sigma \upharpoonright (R_1 \cup F_1)$,

(c) $\nu^{\mathfrak{A}_1} = \nu^{\mathfrak{A}} \upharpoonright (R_1 \cup F_1)$.

If a system $\mathfrak{A}$ of Σ is an expansion of a system $\mathfrak{A}_1$ of Σ_1, then $\mathfrak{A}_1$ is said to be *restriction of the system* $\mathfrak{A}$ to the signature Σ_1 and denoted by $\mathfrak{A} \upharpoonright \Sigma$.

If $\Sigma = \langle r_1^{\mu(r_1)}, \ldots, r_n^{\mu(r_n)}, \ldots; f_1^{\mu(f_1)}, \ldots, f_k^{\mu(f_k)}, \ldots; c_1, \ldots, c_m, \ldots \rangle$, then the algebraic system $\mathfrak{A}$ of the signature Σ will often be designated as follows: $\mathfrak{A} = \langle A, \underline{r_1}, \ldots, \underline{r_n}, \ldots, \underline{f_1}, \ldots, \underline{f_k}, \ldots; \underline{c_1}, \ldots, \underline{c_m}, \ldots \rangle$, where $\underline{r_n}, \underline{f_k}, \underline{c_m}$ denote respectively the relation $\nu^{\mathfrak{A}}(r_n)$, the operation $\nu^{\mathfrak{A}}(f_k)$ and the value of the constant $\nu^{\mathfrak{A}}(c_m)$ on the set A.

EXAMPLE 1. The algebraic system $\mathfrak{N} = \langle N, \underline{+}, \underline{\cdot}; 0, \underline{1} \rangle$, where $N = \omega$ is a set of natural numbers, $\underline{+}$ and $\underline{\cdot}$ are the operations of addition and multiplication, $\underline{0} = 0$, $\underline{1} = 1$, is called an *arithmetic of natural numbers* or simply *arithmetic*. Notice that $\mathfrak{N}$ has no subsystems different from itself. The function signature $\Sigma_1 = \langle +^2, \cdot^2; 0, 1 \rangle$ is called a signature of rings with unity. Not all algebraic systems of Σ_1 are rings. For a system to be a ring it is necessary that the operations should satisfy certain conditions (the axioms for rings). The arithmetic $\mathfrak{N}$ is not a ring and the system $\mathfrak{Z} = \langle Z, \underline{+}, \underline{\cdot}; \underline{0}, \underline{1}\rangle$, where Z is the set of all integers ($Z = \{0, 1, 2, \ldots; -1, -2, \ldots\}$), $\underline{+}$, $\underline{\cdot}$ are the operations of addition and multiplication, $\underline{0} = 0$, $\underline{1} = 1$, is. Notice that $\mathfrak{N} \subseteq \mathfrak{Z}$. The system $\mathfrak{Z}$ is called the *ring of integers*. The system $\mathfrak{R} = \langle R, \underline{+}, \underline{\cdot}; \underline{0}, \underline{1}\rangle$ where R are the real numbers, $\underline{+}$, $\underline{\cdot}$ are operations of addition and multiplication, $\underline{0} = 0$, $\underline{1} = 1$, is also a ring. The system $\mathfrak{Z}$ is a subsystem of $\mathfrak{R}$.

EXAMPLE 2. The function signature $\Sigma_2 = \langle \cdot^2 (^{-1})^1; e\rangle$ is called a group signature. A *group of substitutions of a set X* is a system $\langle S(X), \underline{\cdot}, \underline{(^{-1})}; \underline{e}\rangle$ of the signature Σ_2 where $S(X)$ denotes the set of all distinct-valued mappings of a nonempty set X onto itself, $\underline{\cdot}$ denotes a composition of mappings, $\underline{(^{-1})}$ denotes the inverse of a mapping, e denotes the identity mapping. In general the system $\mathfrak{A} = \langle A, \underline{\cdot}, \underline{(^{-1})}; e\rangle$ of the signature Σ_2 is said to be a *group* if for any $a, a_1, a_2 \in A$ in $\mathfrak{A}$ the following equations hold:

(1) $a \cdot (a_1 \cdot a_2) = (a \cdot a_1) \cdot a_2$,

(2) $a \cdot e = e \cdot a = a$,

(3) $a \cdot a^{-1} = a^{-1} \cdot a = e$,

where $\underline{\cdot}\,(a, a_1)$, $\underline{(^{-1})}(a)$ are briefly written as $a \cdot a_1$ and a^{-1}. If for any $a, a_1 \in A$ in $\mathfrak{A}$ we have in addition equations

(a) $a \cdot a_1 = a_1 \cdot a$,

then the group $\mathfrak{A}$ is said to be an Abelian group. To emphasize that the group $\mathfrak{A}$ is an Abelian group we often replace the symbols $\cdot$, $(^{-1})$ and e by $+$, $(-)$ and 0 respectively. An example of an Abelian group is the group of integers $\langle Z, \underline{+}, \underline{(-)}; \underline{0}\rangle$ where $\underline{+}$ is addition, $\underline{(-)}$ is an operation transforming m into $-m$ and $\underline{0} = 0$.

EXAMPLE 3. If a predicate signature $\Sigma = \langle Q^2\rangle$ of a system $\mathfrak{A}$ consists of a single symbol of a two-place relation Q, then $\mathfrak{A} = \langle A, \underline{Q}\rangle$ is said to be a graph. If $\underline{Q}$ is a partial (linear) ordering on A (see Sec. 11), then $\mathfrak{A}$ is said to be a partially (linearly) ordered set or simply a partial (linear) ordering *. In this case

---

* This definition does not entirely coincide with that of a poset in Sec. 11 (therein the poset is a pair and the graph is a triple); however, by virtue of our convention to denote a graph by $\langle A, P\rangle$, where $P \subseteq A^2$, this will not cause confusion.

$\langle a, b\rangle \in Q$ is denoted by $a \leqslant^{\mathfrak{A}} b$ or simply by $a = b$. A partial ordering $\mathfrak{A}$ is said to be dense if it follows from $a \leqslant b$ and $a \neq b$ that there is $c \in A$ such that $c \neq a$, $c \neq b$, $a \leqslant c$ and $c \leqslant b$. We shall say that two linear orderings $\mathfrak{A}$ and $\mathfrak{B}$ have the *same ends* if the existence in $\mathfrak{A}$ of the first and the last element is equivalent to the existence of the corresponding element in $\mathfrak{B}$. Notice that a subsystem of a partial (linear) ordering is a partial (linear) ordering but a subsystem of a dense linear ordering need not be a dense linear ordering (give a counterexample).

PROPOSITION 4. *If* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are two countable dense linear orderings with the same ends, then* $\mathfrak{A} \simeq \mathfrak{B}$.

PROOF. Let $A = \{a_n \mid n \in \omega\}$, $B = \{b_n \mid n \in \omega\}$. Consider a set G consisting of mappings: $g\colon A_1 \twoheadrightarrow B_1$ satisfying the following conditions:

(1) A_1 and B_1 are finite subsets of A and B respectively;

(2) $g\colon \mathfrak{A}(A_1) \simeq \mathfrak{B}(B_1)$ if $A_1 \neq \varnothing$;

(3) if $|A_1| = 2n > 0$, then $\{a_0, \ldots, a_{n-1}\} \subseteq A_1$ and $\{b_0, \ldots, b_{n-1}\} \subseteq B_1$;

(4) if $|A_1| = 2n + 1$, then $\{a_0, \ldots, a_n\} \subseteq A_1$ and for $n > 0$ $\{b_0, \ldots, b_{n-1}\} \subseteq B_1$;

(5) if $a \in A_1$ is the first (last) element of $\mathfrak{A}$, then ga is the first (last) element of $\mathfrak{B}$.

Since $\varnothing \in G$, we have $G \neq \varnothing$. Let $g\colon A_1 \twoheadrightarrow B_1$ be in G and $|A_1| = 2n$. It follows from condition (3) that we can choose $a \in A \setminus A_1$ for which $\{a_0, \ldots, a_n\} \subseteq A_1 \cup \{a\}$. We take an element $b \in B \setminus B_1$ such that $b \leqslant gc \Leftrightarrow a \leqslant c$ for all $c \in A_1$ and b is the first (last) element in $\mathfrak{B}$ if and only if a is the first (last) element in $\mathfrak{A}$. Such an element exists by virtue of the density of $\mathfrak{B}$ and conditions (2), (5) for g. It is clear that $g \cup \{\langle a, b\rangle\} \in G$. If $|A| = 2n + 1$, then on interchanging $\mathfrak{A}$ and $\mathfrak{B}$ we can find in precisely the same way a pair $\langle a, b\rangle \notin g$ for which $g \cup \{\langle a, b\rangle\} \in G$. Hence there are no maximal elements in the partial ordering $\langle G, \subseteq\rangle$, where $\subseteq$ is the relation of inclusion. Then there is an infinite chain $X \subseteq G$ in G. It follows from conditions (2) to (4) that the union of the elements of X is an isomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$. □

Exercises

1. Show that any algebraic system $\mathfrak{A}$ of a countable signature Σ has a countable or finite subsystem $\mathfrak{B} \subseteq \mathfrak{A}$. (*Hint.* Define at most countable sets B_n, $n \in \omega$, as follows: $B_0 = \{a\}$, where $a \in A$, $B_{n+1} = B_n \cup \{b \mid b$ is the value of the function of $\mathfrak{A}$ on the elements of a set $B_n\}$. Then it is possible to take as the carrier of $\mathfrak{B}$ a set $B = \bigcup\limits_{n \in \omega} B_n$.)

2. For a given algebraic system $\mathfrak{A}$ let $S(\mathfrak{A})$ be the set of its subsystems. Then the system $\langle S(\mathfrak{A}); \underline{\subseteq} \rangle$, where $\langle \mathfrak{B}_1, \mathfrak{B}_2 \rangle \in \underline{\subseteq} \Leftrightarrow \mathfrak{B}_1 \subseteq \mathfrak{B}_2$, is a lattice (see Sec. 11) if the signature Σ of $\mathfrak{A}$ contains symbols of constants.

3. Let $\mathfrak{A}$ have a proper self-isomorphic subsystem. Then $\mathfrak{A}$ has a proper self-isomorphic supersystem.

4. Show that the system $\langle N, \pm \rangle$ has a countable number of subsystems and the system $\langle N; \dot{-} \rangle$ has an uncountable number.

5. Show that if $|\Sigma| < \omega$, then for any $n \in \omega$ there is a finite set X of systems of a signature Σ such that any system of Σ of power n is isomorphic to one of the systems of X.

6. What is the minimal power of the set X in Exercise 5 if Σ contains only $k \in \in \omega$ one-place predicates?

7. Show that the distinct-valued homomorphism $h: A \twoheadrightarrow B$ of a system $\mathfrak{A}$ onto a system $\mathfrak{B}$ of a function signature Σ is an isomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$. Construct an example showing that the condition $R = \varnothing$ on Σ in this exercise cannot be dropped.

16. FORMULAS OF THE SIGNATURE Σ

We fix some countable set $V = \{v_i \mid i \in \omega\}$ whose elements will be called *symbols of variables* or simply *variables* and denoted by the letters x, y and z, possibly with indices. If there occurs a sequence $x_0, \dots, x_n$ of variables in the text, then it is always assumed that $x_i \neq x_j$ for $i \neq j$.

DEFINITION. The set $T(\Sigma)$ of *terms of a signature* $\Sigma = \langle R, F, \mu \rangle$ is defined by induction:

(1) variables $x \in V$ are terms of Σ;

(2) if $t_1, \dots, t_n$ are terms of Σ, $f \in F$ and $\mu(f) = n$, then $f(t_1, \dots, t_n)$ is a term of Σ.

Recall that when $n = 0$ the notation $\Theta(\tau_1, \dots, \tau_n)$ denotes Θ; in particular, it follows from (2) that the symbol $c \in F$ of a constant of Σ is a term of Σ.

Thus terms are words (not all the words, of course) of an alphabet $V \cup F \cup \{(,)\} \cup \{,\}$. The set of variables occurring in a term t is denoted by $FV(t)$. If $FV(t) = \varnothing$, then t is said to be a constant, or closed, term. If t is a term of Σ, then the notation $t(x_1, \ldots, x_n)$ will designate that $FV(t) \subseteq \{x_1, \ldots, x_n\}$. This notation will also be called a term. *

DEFINITION. Let $\mathfrak{A}$ be an algebraic system of a signature Σ. A mapping γ of a set $X \subseteq V$ into A is said to be an *interpretation of variables* of the set X into A. If $FV(t) \subseteq X$ for a term of Σ, then by induction on the length of t we define the *value* $t^{\mathfrak{A}}[\gamma] \in A$ *of the term* t *in* $\mathfrak{A}$ *for the interpretation of* γ:

(1) if $t = x$, $x \in V$, then $t^{\mathfrak{A}}[\gamma] = \gamma x$;

(2) if $t = f(t_1, \ldots, t_n)$, $f \in F$, then $t^{\mathfrak{A}}[\gamma] = \nu^{\mathfrak{A}}(f)(t_1^{\mathfrak{A}}[\gamma], \ldots \ldots, t_n^{\mathfrak{A}}[\gamma])$.

It is clear that if $\gamma_1 \colon X_1 \to A$, $\gamma_2 \colon X_2 \to A$ are two interpretations, $t \in T(\Sigma)$, $FV(t) \subseteq X_1 \cap X_2$ and $\gamma_1 \restriction FV(t) = \gamma_2 \restriction FV(t)$, then $t^{\mathfrak{A}}[\gamma_1] = t^{\mathfrak{A}}[\gamma_2]$. For brevity we shall often write $t^{\mathfrak{A}}(a_1, \ldots \ldots, a_n)$, where $a_1 = \gamma(x_1), \ldots, a_n = \gamma(x_n)$, instead of $t^{\mathfrak{A}}(x_1, \ldots \ldots, x_n)[\gamma]$. If there occurs a notation $t(x_1, \ldots, x_n)$ in the text, then the notation $t^{\mathfrak{A}}(a_1, \ldots, a_n)$, $a_1, \ldots, a_n \in A$ following it will denote $t^{\mathfrak{A}}(x_1, \ldots, x_n)[\gamma]$, where γ is defined as follows: $\gamma\, x_i = a_i$, $i = 1, \ldots, n$.

PROPOSITION 1. (a) *If* $\mathfrak{A}$ *is an algebraic system of a signature* Σ, $X \subseteq A$, $X \neq \varnothing$, *then the carrier* $A(X)$ *of a subsystem* $\mathfrak{A}(X)$ *is equal to a set* $\{t^{\mathfrak{A}}[\gamma] \mid t \in T(\Sigma), \gamma \colon FV(t) \to X\}$.

(b) *If* h *is a homomorphism of an algebraic system* $\mathfrak{A}$ *of* Σ *into a system* $\mathfrak{B}$, $t(x_1, \ldots, x_n) \in T(\Sigma)$ *and* $a_1, \ldots, a_n \in A$, *then* $h(t^{\mathfrak{A}}(a_1, \ldots, a_n)) = t^{\mathfrak{B}}(ha_1, \ldots, ha_n)$.

PROOF. (a) Let $Y = \{t^{\mathfrak{A}}[\gamma] \mid t \in T(\Sigma), \gamma \colon FV(t) \to X\}$. By induction on the length of the term t, if $t(x_1, \ldots, x_n) \in T(\Sigma)$ and $a_1, \ldots, a_n \in X$, then $t^{\mathfrak{A}}(a_1, \ldots, a_n) \in B$ for any subsystem $\mathfrak{B} \subseteq \mathfrak{A}$ for which $X \subseteq B$. It suffices to show therefore that Y is closed under the operations of $\mathfrak{A}$. Let $f \in F$, $\mu(f) = m$, $t_1, \ldots, t_m \in T(\Sigma)$ and $\gamma \colon (FV(t_1) \cup \ldots \cup FV(t_m)) \to X$. Then $\nu^{\mathfrak{A}}(f)(t_1^{\mathfrak{A}}[\gamma], \ldots \ldots, t_n^{\mathfrak{A}}[\gamma]) = t_0^{\mathfrak{A}}[\gamma] \in Y$, where $t_0 = f(t_1, \ldots, t_n)$.

(b) It is easy to prove by induction on the length of t. □

---

* It is not, nor is the letter t, a term of course, but a designation (a "name") of the term.

DEFINITION. A set $F(\Sigma)$ *of formulas of a signature* $\Sigma = \langle R, F, \mu\rangle$ is defined by induction.

(1) If $r \in R$, $\mu(r) = n$ and $t_1, \ldots, t_n \in T(\Sigma)$, then the word $r(t_1, \ldots, t_n)$ is a formula of Σ.

(2) If $t_1, t_2 \in T(\Sigma)$, then the word $t_1 \approx t_2$ is a formula of Σ.

(3) If Φ, Ψ are formulas of Σ, then $(\Phi' \wedge \Psi)$, $(\Phi \vee \Psi)$, $(\Phi \rightarrow \Psi)$ and $\neg \Phi$ are formulas of Σ.

(4) If Φ is a formula of Σ, $x \in V$, then $\forall x\Phi$ and $\exists x\Phi$ are formulas of Σ.

Thus the set $F(\Sigma)$ of formulas of Σ consists of some words of the alphabet $V \cup R \cup F \cup \{\wedge, \vee, \rightarrow \neg, \approx\} \cup \{\forall, \exists\} \cup \{(,)\} \cup \{,\}$. For example, if $r \in R, f, g, c \in F$, $\mu(r) = \mu(g) = 2$, $\mu(f) = 1$, $\mu(c) = 0$, then the word

$$(\forall v_1 \exists v_2 r(v_2, f(v_3)) \vee \neg v_4 \approx g(v_1, c))$$

is a formula of Σ, while the words

$$v_1 \approx v_2 \forall v_1, \quad c \approx v_1 \vee v_2 \approx c,$$
$$(\forall v_1 r(f(v_3), v_2)), \quad (\exists v_1 r(v_1, v_2, v_1) \vee c \approx v_3)$$

are not (why?). The last word is a formula, but of another signature.

A sequence Φ of some symbols is said to be simply a *formula* if it is a formula of some signature. If Φ is a formula, then $\Sigma(\Phi)$ denotes a signature all of whose symbols occur in Φ and Φ is a formula of the signature $\Sigma(\Phi)$. It is clear that $\Sigma(\Phi)$ is uniquely defined by Φ.

A subword of a formula Φ which is itself a formula is called a *subformula* of Φ. Formulas of the form $r(t_1, \ldots, t_n)$ and $t_1 \approx t_2$, where r is a predicate symbol, t_1, t_2 are terms, are called *atomic* *. Atomic formulas containing at most one signature symbol are called *atomical*. Thus an atomic formula of a signature Σ has one of the following forms:

$$v_i \approx v_j, \quad c \approx v_i, \quad v_i \approx c, \quad v_j \approx f(v_{i_0}, \ldots, v_{i_n}),$$
$$f(v_{i_0}, \ldots, v_{i_n}) \approx v_j, \quad r(v_{i_0}, \ldots, v_{i_n}), r,$$

---

* In some books such formulas are called elementary, but we shall not use this term.

where c is a constant, f is a function symbol and r is a predicate symbol of Σ. The sign $\approx$ is the *equality symbol* or simply equality. The signs $\forall$ and $\exists$ are called the *universal* and *existential quantifiers* respectively. The notation $\forall x$ ($\exists x$) stands for "for all x" ("there is an x"). A formula containing no quantities is called a quantifier-free formula.

The proof of the following three propositions is essentially a repetition of the proofs of Propositions 2.1, 2.2 and Corollary 2.1 respectively. (Considering cases where a formula begins with quantifiers does not differ essentially from considering in the proposition pointed out the case where a formula begins with a negation.)

PROPOSITION 2. *Any nonatomic formula Φ of a signature Σ is representable in one and only one of the following forms:*

$$(\Psi \wedge X), \quad (\Psi \vee X), \quad (\Psi \rightarrow X), \quad \forall x \, \Psi, \exists x \, \Psi \quad \text{or} \quad \neg \Psi$$

for uniquely defined formulas Ψ and X of the signature Σ. ☐

PROPOSITION 3. *If Φ is a formula of a signature Σ and η and θ are occurrences in Φ of subformulas of Ψ and X respectively, then either η and θ have no symbol occurrences or one of them is contained entirely in the other.* ☐

PROPOSITION 4. *Uniquely associated with each occurrence in a formula Φ of a signature Σ of the symbols (, $\neg$, $\forall$ or $\exists$ is some occurrence of a subformula of Φ whose first symbol is the occurrence in question of the corresponding symbol.* ☐

DEFINITION. A subformula of a formula Φ of a signature Σ associated, by Proposition 4, with an occurrence of a quantifier $\forall$ ($\exists$) is called the *scope of that occurrence of the quantifier* $\forall$ ($\exists$).

In what follows we shall use our convention to drop outer brackets (Sec. 2). Notice that a formula of the propositional calculus may be regarded as a formula of some signature if it is assumed that the symbols of propositional variables are 0-place predicate symbols.

DEFINITION. For each formula Φ of a signature Σ we define a set $FV(\Phi)$ of *free variables of the formula* Φ as follows.

(1) If Φ is an atomic formula of the form r, $r(t_1, \ldots, t_n)$ or $t_1 \approx t_2$, then the set $FV(\Phi)$ is equal to $\varnothing$, $FV(t_1) \cup \ldots \cup FV(t_n)$ or $FV(t_1) \cup FV(t_2)$ respectively.

(2) If $\Phi = \neg\Psi$, then $FV(\Phi) = FV(\Psi)$.

(3) If $\Phi = \Phi_1 \tau \Phi_2$, where $\tau \in \{\wedge, \vee, \rightarrow\}$, then $FV(\Phi) = FV(\Phi_1) \cup FV(\Phi_2)$.

(4) If $\Phi = Qx\Psi$, where $Q \in \{\forall, \exists\}$, then $FV(\Phi) = FV(\Psi) \setminus \{x\}$.

It is clear that for any formula Φ it is possible to find all the elements of $FV(\Phi)$ in a finite number of steps.

An occurrence η of a variable x in a formula Φ of Σ is said to be *bound* if η is in the scope of some occurrence of the quantifier $\forall$ or $\exists$ immediately followed by the symbol x. If the occurrence η of a variable x in Φ is not bound, then it is said to be *free*. If Φ contains free (bound) occurrences of a variable x, we shall say that x *occurs free* (*bound*) in Φ.

PROPOSITION 5. *If Φ is a formula of Σ then a variable x is in $FV(\Phi)$ if and only if there is a free occurrence of x in Φ.*

The proof is easy to carry out by induction on the length of Φ and it will be left to the reader. □

If Φ is a formula, then in what follows $\Phi(x_1, \ldots, x_n)$ will denote the formula Φ and the fact that $FV(\Phi) \subseteq \{x_1, \ldots, x_n\}$.

Now we define the main notion of this chapter.

DEFINITION. For an algebraic system $\mathfrak{A}$ of a signature Σ an interpretation of variables $\gamma: X \rightarrow A$ and a formula $\Phi \in F(\Sigma)$ such that $FV(\Phi) \subseteq X$ we define a relation $\mathfrak{A} \models \Phi[\gamma]$ (for "$\Phi[\gamma]$ *is true in* $\mathfrak{A}$") by induction on the length of Φ.

(1) If $\Phi = r$, $r \in R$, $\mu(r) = 0$, then $\mathfrak{A} \models \Phi[\gamma]$ is equivalent to $\varnothing \in \nu^{\mathfrak{A}}(r)$.

(2) If $\Phi = r(t_1, \ldots, t_n)$, $r \in R$, $\mu(r) = n$, $t_1, \ldots, t_n \in T(\Sigma)$, then $\mathfrak{A} \models \Phi[\gamma]$ is equivalent to $\langle t_1^{\mathfrak{A}}[\gamma], \ldots, t_n^{\mathfrak{A}}[\gamma]\rangle \in \nu^{\mathfrak{A}}(r)$ *.

(3) If Φ is equal to $t_1 \approx t_2$, $t_1, t_2 \in T(\Sigma)$, then $\mathfrak{A} \models \Phi[\gamma]$ is equivalent to $t_1^{\mathfrak{A}}[\gamma] = t_2^{\mathfrak{A}}[\gamma]$.

(4) If $\Phi = \neg\Psi$, then $\mathfrak{A} \models \Phi[\gamma]$ if and only if it is false say that $\mathfrak{A} \models \Psi[\gamma]$.

(5) If $\Phi = (\Phi_1 \wedge \Phi_2)$, then $\mathfrak{A} \models \Phi[\gamma] \Leftrightarrow (\mathfrak{A} \models \Phi_1[\gamma]$ and $\mathfrak{A} \models \Phi_2[\gamma])$.

---

* Of course, (2) includes (1), since we have agreed to assume $r(t_1, \ldots, t_n)$ equal to r when $n = 0$. We have included (1) here to emphasize the peculiarity of 0-place predicates.

(6) If $\Phi = (\Phi_1 \vee \Phi_2)$, then $\mathfrak{A} \models \Phi[\gamma] \Leftrightarrow (\mathfrak{A} \models \Phi_1[\gamma]$ or $\mathfrak{A} \models \Phi_2[\gamma])$.

(7) If $\Phi = (\Phi_1 \to \Phi_2)$, then $\mathfrak{A} \models \Phi[\gamma] \Leftrightarrow$ (if $\mathfrak{A} \models \Phi_1[\gamma]$, then $\mathfrak{A} \models \Phi_2[\gamma]$).

(8) If $\Phi = \exists x \Psi$, then $\mathfrak{A} \models \Phi[\gamma]$ if and only if there is an interpretation $\gamma_1 : X_1 \to A$ such that $x \in X_1$, $\gamma_1 \restriction FV(\Phi) = \gamma \restriction FV(\Phi)$ and $\mathfrak{A} \models \Psi[\gamma_1]$.

(9) If $\Phi = \forall x \Psi$, then $\mathfrak{A} \models \Phi[\gamma]$ if and only if for any interpretation $\gamma_1 : X_1 \to A$ such that $x \in X_1$ and $\gamma_1 \restriction FV(\Phi) = \gamma \restriction FV(\Phi)$ we have $\mathfrak{A} \models \Psi[\gamma_1]$.

It is obvious from this definition that free and bound occurrences of variables in a formula Φ of Σ play quite different roles in establishing the truth of the formula. Namely, free occurrences of a variable x are "assigned" a constant value $\gamma(x)$ while bound occurrences are not "assigned" any constant values and instead all possible values of them are considered.

PROPOSITION 6. *Let* $\mathfrak{A}$ *be an algebraic system of a signature* Σ *and* $\Phi \in F(\Sigma)$. *If* $\gamma_1 : X_1 \to A$, $\gamma_2 : X_2 \to A$ *are two interpretations for which* $FV(\Phi) \subseteq X_1 \cap X_2$ *and* $\gamma_1 \restriction FV(\Phi) = \gamma_2 \restriction FV(\Phi)$, *then* $\mathfrak{A} \models \Phi[\gamma_1] \Leftrightarrow \mathfrak{A} \models \Phi[\gamma_2]$.

Proof is easy to carry out by induction on the length of Φ. □

Instead of $\mathfrak{A} \models \Phi(x_1, \ldots, x_n)[\gamma]$ we shall often use a more convenient notation $\mathfrak{A} \models \Phi(a_1, \ldots, a_n)$, where $a_1 = \gamma(x_1), \ldots, a_n = \gamma(x_n)$. Namely, if a notation $\Phi(x_1, \ldots, x_n)$ occurs in the text, then the notation $\mathfrak{A} \models \Phi(a_1, \ldots, a_n)$, $a_1, \ldots, a_n \in A$ following it will denote $\mathfrak{A} \models \Phi(x_1, \ldots, x_n)[\gamma]$, where γ is defined as follows: $\gamma x_i = a_i$, $i = 1, \ldots, n$. Such an abbreviation is possible by Proposition 6.

DEFINITION. If Φ is a formula of a signature Σ and $FV(\Phi) = \varnothing$, then Φ is said to be a *closed formula* or a *sentence*.

If Φ is a sentence of a signature Σ, $\mathfrak{A}$ is a system of Σ, then the relation $\mathfrak{A} \models \Phi[\gamma]$ is independent of the interpretation γ and we shall denote it simply as $\mathfrak{A} \models \Phi$. It is also clear that if for a formula Φ, a system $\mathfrak{A}$ and an interpretation γ a relation $\mathfrak{A} \models \Phi[\gamma]$ is defined, then $\mathfrak{A} \models \Phi[\gamma] \Leftrightarrow \mathfrak{A} \restriction \Sigma(\Phi) \models \Phi[\gamma]$. If $\Phi[\gamma]$ is not true in $\mathfrak{A}$, then we say that $\Phi[\gamma]$ is *false in* $\mathfrak{A}$.

DEFINITION. A formula Φ is said to be *identically true or valid if* $\mathfrak{A} \models \Phi[\gamma]$ for any system $\mathfrak{A}$ of a signature $\Sigma(\Phi)$ and any interpretation $\gamma\colon FV(\Phi) \to A$. It is clear that in this definition the signature $\Sigma(\Phi)$ may be substituted for by any $\Sigma \supseteq \Sigma(\Phi)$. A set of formulas $Y \subseteq F(\Sigma)$ is said to be *satisfiable in a system* $\mathfrak{A}$ of a signature Σ if there is an interpretation $\gamma\colon \bigcup\limits_{\Phi \in Y} FV(\Phi) \to A$ such that $\mathfrak{A} \models \Phi[\gamma]$ for all $\Phi \in Y$. A formula Φ is said to be *satisfiable in a system* $\mathfrak{A}$ if a set $\{\Phi\}$ is satisfiable in $\mathfrak{A}$.

The notion of the truth of a formula on a system belongs to the basic concepts of mathematical logic along with the notion of derivability. The importance of this notion is due to the fact that many theorems in mathematics can be expressed as statements about the truth of some formula on algebraic systems from some class. In contrast to the properties of "being a formula" and of "being an identically true formula of PC", in the general case there is no effective method that would allow us to establish for a sentence Φ in a finite number of steps if $\mathfrak{A} \models \Phi$ is true. This is due to the fact that if A is infinite, then (8) and (9) require checking an infinite number of conditions *. In the general case (2) and (3) are not "effective" either, since the predicates and functions of an infinite system $\mathfrak{A}$ may not be given "effectively".

Now we establish a simple but important fact.

PROPOSITION 7. *If f is an isomorphism of a system $\mathfrak{A}$ onto a system $\mathfrak{B}$, $\Phi(x_1, \ldots, x_n)$ is a formula of the signature of $\mathfrak{A}$, then for any $a_1, \ldots, a_n \in A$ the property $\mathfrak{A} \models \Phi(a_1, \ldots, a_n)$ is equivalent to $\mathfrak{B} \models \Phi(fa_1, \ldots, fa_n)$. In particular, if Φ is a sentence, then $\mathfrak{A} \models \Phi$ is equivalent to $\mathfrak{B} \models \Phi$.*

Proof is easy to carry out by induction on the length of Φ. If Φ is an atomic formula, then the statement follows from the definition of an isomorphism and Proposition 1(b). The induction step will be left as an exercise to the reader. □

In contrast to infinite systems, the truth of a formula Φ on a finite system $\mathfrak{A}$ of $\Sigma(\Phi)$ can be verified in a finite number of steps. This is easily shown by induction on the length of Φ.

DEFINITION. Let $n \in \omega$, $n > 0$. A sentence Φ is said to be *n-valid* if $\mathfrak{A} \models \Phi$ for any algebraic system $\mathfrak{A}$ of power n and a signature $\Sigma(\Phi)$.

---

* It will be shown in Chapter 7 that this difficulty cannot be avoided.

PROPOSITION 8. *There is an effective procedure (an algorithm) allowing one to establish for any* $n \in \omega$, $n > 0$, *and any sentence* Φ *in a finite number of steps whether or not* Φ *is n-valid.*

PROOF. It is obvious that for a finite set X the sets $P(X)$ and X^n, $n \in \omega$, are finite. For any finite signature Σ, therefore, there is only a finite number of systems of Σ with a finite carrier X. The procedure for verifying n-validity reduces to writing out all the systems of $\Sigma(\Phi)$ with carrier $\{1, 2, \ldots, n\}$ and verifying the truth of Φ on each of the systems written out. As noted above, such a verification is carried out in a finite number of steps. $\square$

In a similar way to n-validity, $0 < n < \omega$, one can define the $\varkappa$-validity of a formula Φ for an infinite cardinal $\varkappa$. As is to be shown in Sec. 24, these concepts coincide for all infinite cardinals $\varkappa$. What other relations are there between the two concepts? As is shown in the next section, if a sentence Φ is infinitely valid, then there is a number $n_0 \in \omega$ such that Φ is k-valid for any $k \geqslant n_0$. The n-validity of a sentence Φ for any $n \in \omega$, $n \neq 0$, does not in general imply (Exercise 4) the validity of Φ. Note that no complete description of the set

$$S = \{X \subseteq \omega \mid X \text{ is equal to } \{n \mid \Phi \text{ is } n\text{-valid}\} \text{ for some sentence } \Phi\}$$

has yet been obtained. It is not even known if the set S is closed under the complement in the set ω. We note here a simple fact.

PROPOSITION 9. *For any* $n \in \omega$, $n \geqslant 1$, *there is a sentence* Φ_n *of an empty signature* Σ_0 (i. e. $\Sigma_0 = \langle \emptyset, \emptyset \rangle$) *such that* Φ_n *is n-valid and* $\neg \Phi_n$ *is k-valid for any* $k \neq n$, $k \geqslant 1$.

PROOF. We may choose as Φ_n a sentence

$$\exists v_1 \ldots \exists v_n((\neg\, v_1 \approx v_2 \wedge (\neg\, v_1 \approx v_3 \wedge (\ldots \wedge \neg$$
$$\neg\, v_{n-1} \approx v_n)\ldots)) \wedge \forall v_0(v_0 \approx v_1 \vee (\ldots \vee v_0 \approx v_n)\ldots)). \square$$

The formula $\forall v_1 \forall v_2(P(v_1) \rightarrow P(v_2))$ contains no equality and function symbols, is 1-valid and is not n-valid for $n > 1$. Also easily constructed (Exercise 3) is a formula Ψ_n without equality and functions, which is k-valid for $0 < k \leqslant n$ and which is not m-valid for $m > n$. It is impossible to construct the formula Φ_n of Proposition 9 without equality and functions in view of the following fact (Exercise 5): if a sentence Φ contains no equality and function symbols, then the n-validity of Φ implies the k-validity of Φ for any $k \leqslant n$, $k \neq 0$.

Exercises

1. Show that for any finite signature Σ there is a procedure for determining from any finite sequence of symbols whether or not it is a formula of Σ.

2. Let h be a homomorphism of a system $\mathfrak{A}$ of a signature Σ into a system $\mathfrak{B}$. Then for any atomic $\Phi(x_1, \ldots, x_n) \in F(\Sigma)$ and any $a_1, \ldots, a_n \in A$ we have $\mathfrak{A} \vDash \Phi(a_1, \ldots, a_n) \Rightarrow \mathfrak{B} \vDash \Phi(ha_1, \ldots, ha_n)$.

3. Show that the following formula Ψ_n is k-valid if and only if $1 \leqslant k \leqslant n$:

$$\exists v_2 \ldots \exists v_{n+1} \forall v_0 (\forall v_1 (r(v_2, v_1) \to r(v_0, v_1)) \vee \\ \vee (\ldots \vee \forall v_1 (r(v_{n+1}, v_1) \to r(v_0, v_1))\ldots)).$$

4. Show that the following formula is n-valid for any $n \in \omega$, $n \neq 0$, and is not simply valid:

$$\exists v_0 \forall v_1 \neg f(v_1) \approx v_0 \to \exists v_0 \exists v_1 (f(v_0) \approx f(v_1) \wedge \neg v_0 \approx v_1).$$

5. Suppose $0 < k < n < \omega$, a sentence Φ is n-valid and contains no equality and function symbols. Then Φ is k-valid. (*Hint*. Let $\mathfrak{A} \vDash \neg \Phi$, where $\mathfrak{A}$ is a system of a signature $\Sigma(\Phi)$ with carrier $\{1, 2, \ldots, k\}$. Construct a system $\mathfrak{B} \supseteq \mathfrak{A}$ of power n by defining on a set $B = \{1, 2, \ldots, n\}$ predicates r of $\Sigma(\Phi)$ as follows:

$$\langle i_1, \ldots, i_m \rangle \in \gamma^{\mathfrak{B}}(r) \Leftrightarrow \langle j_1, \ldots, j_m \rangle \in \nu^{\mathfrak{A}}(r),$$

where $j_s = i_s$ if $i_s \leqslant k$ and $j_s = k$ otherwise. Then $\mathfrak{B} \vDash \neg \Phi$.)

17. COMPACTNESS THEOREM

The compactness theorem was proved by A. I. Maltsev in 1936. It was also he who was the first to show its importance as a new method for proving not only theorems of mathematical logic but also those of algebra. We shall give a proof of the theorem via ultraproducts introduced by Los' in 1955.

Given a family of sets $S = \{X_i \mid i \in I\}$ the *Cartesian product* of S is the set

$$I\text{-prod}\, X_i = \{f: I \to \bigcup_{i \in I} X_i \mid fi \in X_i\}.$$

For $j \in I$, a mapping of I-prod X_i into X_j assigning to an element f an element $f(j)$ is called a *projection* of the Cartesian product on the jth coordinate and denoted by the same letter j.

Given a filter D on I we define on I-prod X_i a relation $\overset{D}{\sim}$ as follows:

$$f \overset{D}{\sim} g \Leftrightarrow \{i \mid fi = gi\} \in D.$$

LEMMA 1. *A relation* $\overset{D}{\sim}$ *is an equivalence on* I-prod X_i.

PROOF. The reflexivity and symmetry of $\overset{D}{\sim}$ are obvious. Let $f \overset{D}{\sim} g$ and $g \overset{D}{\sim} h$. Then the set $Y = \{i \mid fi = hi\}$ contains the intersection of the sets $\{i \mid fi = gi\}$ and $\{i \mid gi = hi\}$ which are elements of D. It follows from (2) and (3) that $Y \in D$. □

A mapping assigning to an element $f \in I$-prod X_i a $\overset{D}{\sim}$-equivalence class containing f will be denoted by the same letter D as the filter. The set

$$D_I\text{-prod}\, X_i = \{Df \mid f \in I\text{-prod}\, X_i\}$$

is called a *D-filtered product of sets* X_i, $i \in I$.

DEFINITION. *A D-filtered product of a family of algebraic systems* $\{\mathfrak{A}_i \mid i \in I\}$ *of a signature* Σ *is an algebraic system* $\mathfrak{A} = D$-prod $\mathfrak{A}_i$ of Σ with carrier $A = D$-prod A_i and the following interpretation $\nu^{\mathfrak{A}}$ of Σ in $\mathfrak{A}$.

(1) If $c \in F$ and $\mu(c) = 0$, then for $f \in I$-prod A_i

$$Df = \nu^{\mathfrak{A}}(c) \Leftrightarrow \{i \mid fi = \nu^{\mathfrak{A}_i}(c)\} \in D.$$

2. If $s \in R \cup F$, then for $f_1, \ldots, f_n \in I$-prod A_i $\langle Df_1, \ldots, Df_n\rangle \in \nu^{\mathfrak{A}}(s) \Leftrightarrow \{i \mid \langle f_1 i, \ldots, f_n i\rangle \in \nu^{\mathfrak{A}_i}(s)\} \in D$, where $n = \mu(s)$ if $s \in R$ and $n = \mu(s) + 1$ if $s \in F$.

We verify that this definition is correct, i. e. that the sets $\nu^{\mathfrak{A}}(s)$ and $\nu^{\mathfrak{A}}(c)$ are independent of the choice of representatives $f_1, \ldots, f_n$ and f in the classes $Df_1, \ldots, Df_n$ and Df. Indeed, let $Y_k = \{i \mid f_k i = g_k i\} \in D$, $1 \leqslant k \leqslant n$. The sets $W_1 = \{i \mid \langle f_1 i, \ldots, f_n i\rangle \in \nu^{\mathfrak{A}_i}(s)\}$ and $W_2 = \{i \mid \langle g_1 i, \ldots, g_n i\rangle \in \nu^{\mathfrak{A}_i}(s)\}$ have the same intersections with the element $Y_1 \cap \ldots \cap Y_n$ of the filter D. Hence $W_1 \in D \Leftrightarrow W_2 \in D$. The correctness of (1) is similarly shown. To state that $\mathfrak{A}$ is a system of a signature Σ it is in addition necessary to show that $\nu^{\mathfrak{A}}(s)$ is an operation on A if $s \in F$. Let $s \in F$ and $\mu(s) = n$. For elements $f_1, \ldots, f_n \in I$-prod A_i we define $f \in I$-prod A_i as follows: $fi = \nu^{\mathfrak{A}_i}(s)(f_1 i, \ldots, f_n i)$, $i \in I$. Then $\langle Df_1, \ldots, Df_n, Df\rangle \in \nu^{\mathfrak{A}}(s)$. Suppose that for some $g \in I$-prod A_i we have

$$\langle Df_1, \ldots, Df_n, Dg\rangle \in \nu^{\mathfrak{A}}(s).$$

Since $\nu^{\mathfrak{A}_i}(s)$, $i \in I$, are functions, the set $\{i \mid fi = gi\}$ contains the intersections of the sets $\{i \langle f_1 i, \ldots, f_n i, fi\rangle \in \nu^{\mathfrak{A}_i}(s)\}$ and $\{i \mid \langle f_1 i, \ldots, f_n i, gi\rangle \in \nu^{\mathfrak{A}_i}(s)\}$ which are in D. Hence $Df = Dg$.

A filtered product $\{I\}$-prod $\mathfrak{A}_i$ is called a *Cartesian* or *direct product* of systems $\mathfrak{A}_i$, $i \in I$. We give an independent definition to this important special case. Let $\mathfrak{A} = I$-prod $\mathfrak{A}_i$ be a system of a signature Σ with carrier $A = I$-prod A_i and the following interpretation of Σ in A.

(1) If $c \in F$ and $\mu(c) = 0$, then

$$\nu^{\mathfrak{A}}(c)(i) = \nu^{\mathfrak{A}_i}(c).$$

(2) If $s \in R \cup F$, then

$$\langle f_1, \ldots, f_n\rangle \in \nu^{\mathfrak{A}}(s) \Leftrightarrow \langle f_1 i, \ldots, f_n i\rangle \in \nu^{\mathfrak{A}_i}(s) \qquad \text{for all} \quad i \in I,$$

where $n = \mu(s)$ if $s \in R$ and $n = \mu(s) + 1$ if $s \in F$.

It is clear that a mapping assigning to an element f an element $\{f\}$ is an isomorphism of I-prod $\mathfrak{A}_i$ onto $\{I\}$-prod $\mathfrak{A}_i$ and so without fear of confusion the system I-prod $\mathfrak{A}_i$ will also be called a Cartesian of direct product. A Cartesian product I-prod $\mathfrak{A}_i$ is often denoted by $\prod\limits_{i \in I} \mathfrak{A}_i$ or by $\mathfrak{A}_{i_1} \times \ldots \times \mathfrak{A}_{i_n}$ if $I = \{i_1, \ldots, i_n\}$ is a finite set. We point out a simple but useful fact relating Cartesian products to filtered products.

PROPOSITION 1. *For any filter D on I and any systems $\{\mathfrak{A}_i \mid i \in I\}$ of a signature Σ a mapping D: I-prod $A_i \twoheadrightarrow D$-prod A_i is a homomorphism of a system $\mathfrak{A} = I$-prod $\mathfrak{A}_i$ onto a system $\mathfrak{A}' = D$-prod $\mathfrak{A}_i$.*

PROOF. Suppose $s \in R \cup F$ is not a constant and $\langle f_1, \ldots, f_n\rangle \in \nu^{\mathfrak{A}}(s)$. By the definition of a Cartesian product $\{i \mid \langle f_1 i, \ldots, f_n i\rangle \in \nu^{\mathfrak{A}_i}(s)\} = I$. Since $I \in D$, we have $\{i \mid \langle f_1 i, \ldots, f_n i\rangle \in \nu^{\mathfrak{A}_i}(s)\} \in D$, i. e. $\{Df_1, \ldots, Df_n\rangle \in \nu^{\mathfrak{A}'}(s)$. The case where s is a constant is similar. □

In what follows, by a *class* we mean some property Θ of sets *. Sets satisfying a property Θ are elements of the class Θ. In particular, all sets form a class V which is not a set. The property of "being an element of a set X" defines the set X and so any set may be thought of as a class. Of course, one cannot treat classes as sets, one cannot, for example, consider the class of all subclasses of a given class K. However, if K_1, K_2 are classes, then one can define in an obvious way the classes $K_1 \cap K_2$, $K_1 \cup K_2$ and $K_1 \setminus K_2$. If a is an element of K, then just as in the case of sets we shall say that a is a member of K or is in K and write $a \in K$.

---

* Since we have assumed ZFC to be a basis, by a property Θ we mean a property denoted by the formula $\Phi(x, y_1, \ldots, y_n)$ of the signature $\langle \in^2 \rangle$, where the variables $y_1, \ldots, y_n$ are parameters. As a "code" of a class K defined via parameters $a_1, \ldots, a_n$ one may take a set $\langle\langle y_1, a_1\rangle, \ldots, \langle y_n, a_n\rangle, \Phi(x, y_1, \ldots, y_n)\rangle$, where $\Phi(x, y_1, \ldots, y_n)$ is a formula of the signature $\langle \in^2 \rangle$ for which $\Phi(b, a_1, \ldots, a_n) \Leftrightarrow$ (b is an element of K).

Given some class K of algebraic systems of a signature Σ and a filter D on I, we say that *K is closed under the D-filtered products* if for any set $\{\mathfrak{A}_i \mid i \in I\}$ of systems in K we have $D\text{-prod}\,\mathfrak{A}_i \in K$. If for $\Phi(x_1, \ldots, x_n) \in F(\Sigma)$ we define $K(\Phi)$ to be a class of systems $\mathfrak{A}$ of a signature Σ such that for all $a_1, \ldots, a_n \in A$ in $\mathfrak{A}$ $\Phi(a_1, \ldots, a_n)$ is true, then it is easily verified that for an atomic formula Φ the class $K(\Phi)$ is closed under any Cartesian products. By Proposition 1 and Exercise 16.2 $K(\Phi)$ is also closed under all filtered products for an atomic formula Φ. As is to be shown in what follows, this is true not only for atomic formulas. If, however, D is an ultrafilter, then for any formula $\Phi \in F(\Sigma)$ the class $K(\Phi)$ is closed under D-filtered products (Theorem 1 below).

DEFINITION. A formula $\Phi(x_1, \ldots, x_n)$ is said to be *D-filtering* (on a set I) if for any set $\{\mathfrak{A}_i \mid i \in I\}$ of algebraic systems of a signature $\Sigma(\Phi)$ and any $Df_1, \ldots, Df_n \in D\text{-prod}\,A_i$

$$D\text{-prod}\,\mathfrak{A}_i \vDash \Phi(Df_1, \ldots, Df_n) \Leftrightarrow$$
$$\Leftrightarrow \{i \mid \mathfrak{A}_i \vDash \Phi(f_1 i, \ldots, f_n i)\} \in D.$$

If in this definition the implication $\Leftarrow$ holds instead of $\Leftrightarrow$, then the formula Φ is said to be *conditionally D-filtering*. A formula Φ is said to be *(conditionally) filtering* if it (conditionally) filters for any filter D.

If γ is an interpretation of some set of variables in $I\text{-prod}\,A_i$, then by $D(\gamma)$ we denote the composition of γ and D. By $i(\gamma)$ we denote the composition of γ and the projection on the ith coordinate.

LEMMA 2. *If Φ and Ψ (conditionally) D-filter, then formulas $\forall x \Phi$, $\exists x \Phi$ and $\Phi \wedge \Psi$ (conditionally) D-filter.*

PROOF. Fix some interpretation γ of free variables of a formula $\forall x \Phi$ in the set $I\text{-prod}\,A_i$.

Let $\{i \mid \mathfrak{A}_i \models \forall x\Phi[i(\gamma)]\} \in D$. Then for any $f \in I$-prod A_i, if we consider $\gamma' \supseteq \gamma$ such that $\gamma'(x) = f$, we have

$$\{i \mid \mathfrak{A}_i \models \Phi[i(\gamma')]\} \in D.$$

If Φ conditionally filters, then D-prod $\mathfrak{A}_i \models \Phi[D(\gamma')]$ for any γ': $FV(\Phi) \to I$-prod A_i, $\gamma \subseteq \gamma'$, i. e. D-prod $\mathfrak{A}_i \models \forall x\Phi[D(\gamma)]$.

Suppose D-prod $\mathfrak{A}_i \models \forall x\Phi[D(\gamma)]$ and Φ filters. Consider a set $X = \{i \mid \mathfrak{A}_i \models \forall x\Phi[i(\gamma)]\}$. Choose a function $f \in I$-prod A_i such that for $i \in I \setminus X$ we have $\mathfrak{A}_i \models \neg\, \Phi[i(\gamma')]$, where $\gamma' \supseteq \gamma$, $\gamma'(x) = f$. Then from the fact that Φ filters and from D-prod $\mathfrak{A}_i \models$ $\models \Phi[D(\gamma')]$ it follows that $X = \{i \mid \mathfrak{A}_i \models \Phi[i(\gamma')]\} \in D$.

The cases of $\exists x\Phi$ and $\Phi \wedge \Psi$ are similar and they will be left as exercises to the reader. ☐

LEMMA 3. *Atomic formulas filter for any filter D.*

PROOF. Let $\Phi(x_1, \ldots, x_n)$ be an atomic formula of the form $s(t_1, \ldots, t_m)$, where $s \in R$, $\mu(s) = m$, $t_1, \ldots, t_m$ are terms, let $\gamma\colon \{x_1, \ldots, x_n\} \to I$-prod A_i be an interpretation of variables and $f_i = \gamma(x_i)$, $i \in \{1, \ldots, n\}$. Then for $\mathfrak{A} = D$-prod $\mathfrak{A}_i$

$$\mathfrak{A} \models \Phi(Df_1, \ldots, Df_n) \Leftrightarrow \langle t_1^{\mathfrak{A}}[\gamma D], \ldots, t_m^{\mathfrak{A}}[\gamma D]\rangle \in \nu^{\mathfrak{A}}(s).$$

By Proposition 1 and 16.1(b) we have $t_j^{\mathfrak{A}}[\gamma D] = Dt_j^{\mathfrak{B}}[\gamma]$, $1 \leqslant j \leqslant$ $\leqslant m$, where $\mathfrak{B} = I$-prod $\mathfrak{A}_i$ and so

$$\langle t_1^{\mathfrak{A}}[\gamma D], \ldots, t_m^{\mathfrak{A}}[\gamma D]\rangle \in \nu^{\mathfrak{A}}(s) \Leftrightarrow \langle Dt_1^{\mathfrak{B}}[\gamma], \ldots$$
$$\ldots, Dt_m^{\mathfrak{B}}[\gamma]\rangle \in \nu^{\mathfrak{A}}(s) \Leftrightarrow \{i \mid \langle t_1^{\mathfrak{B}}[\gamma](i), \ldots, t_m^{\mathfrak{B}}[\gamma](i)\rangle \in \nu^{\mathfrak{A}_i}(s)\} \in D.$$

But $t_j^{\mathfrak{B}}[\gamma](i) = [t_j^{\mathfrak{B}}(f_1, \ldots, f_n)](i) = t_j^{\mathfrak{A}_i}(f_1 i, \ldots, f_n i)$ and so

$$\langle t_1^{\mathfrak{B}}[\gamma](i), \ldots, t_m^{\mathfrak{B}}[\gamma](i)\rangle \in \nu^{\mathfrak{A}_i}(s) \Leftrightarrow \mathfrak{A}_i \models \Phi(f_1 i, \ldots, f_n i).$$

Thus

$$D\text{-prod } \mathfrak{A}_i \models \Phi(Df_1, \ldots, Df_n) \Leftrightarrow \{i \mid \mathfrak{A}_i \models \Phi(f_1 i, \ldots, f_n i)\} \in D.$$

The case where Φ has the form $t_1 \approx t_2$ is similar. ☐

THEOREM 1. (ŁOS'). *Any formula Φ filters for any ultrafilter D.*

PROOF. By induction on the length of Φ. Since the truth of the formulas $\Phi \to \Psi$ and $\Phi \vee \Psi$ is equivalent to that of $\neg(\Phi \wedge \neg\Psi)$ and $\neg(\neg\Phi \wedge \neg\Psi)$ respectively, by Lemmas 2 and 3 it suffices to show that $\neg\Phi$ D-filters for a D-filtering formula Φ. The property

$\varnothing \notin D$ and Proposition 12.2 yield $X \notin D \Leftrightarrow I \setminus X \in D$. Therefore, from the fact that Φ filters we get

$$D\text{-prod}\,\mathfrak{A}_i \models \neg\Phi[\gamma] \Leftrightarrow \{i \mid \mathfrak{A}_i \models \Phi[\gamma i]\} \notin$$
$$\notin D \Leftrightarrow \{i \mid \mathfrak{A}_i \models \neg\Phi[\gamma i]\} \in D. \ \square$$

DEFINITION. An algebraic system $\mathfrak{A}$ of a signature Σ is said to be a *model of a set of formulas* Γ of Σ if there is an interpretation γ in A of variables occurring free in the elements of Γ such that $\mathfrak{A} \models \Phi[\gamma]$ for all $\Phi \in \Gamma$. The set Γ is said to be *satisfiable* if Γ has a model. The set is said to be *locally satisfiable* if each finite subset of Γ has a model.

As a consequence of Theorem 1 we obtain the following very important theorem known as the *compactness theorem*.

THEOREM 2. *Every locally satisfiable set* Γ *of a signature* Σ *is satisfiable.*

PROOF. Consider a set I of finite subsets of Γ. For $i \in I$ choose systems $\mathfrak{A}_i$ of Σ and interpretations γ_i in A_i of free variables occurring in the formulas of i such that $\mathfrak{A}_i \models \Phi[\gamma_i]$ for all $\Phi \in i$. For $i \in I$, consider sets $X_i = \{j \in I \mid i \subseteq j\}$. The system of sets $\{X_i \mid i \in I\}$ is a family of sets with finite intersection property. Indeed, if $i_0, \ldots, i_k \in I$ and $j = i_0 \cup \ldots \cup i_k$, then $j \in X_{i0} \cap \ldots \cap X_{ik}$. By Proposition 12.1 there is an ultrafilter D such that $X_i \in D$ for all $i \in I$. For a variable x occurring free in some element of Γ we define $\gamma(x) \in I\text{-prod}\,A_i$ as follows:

$$\gamma(x)(i) = \begin{cases} \gamma_i(x) \text{ if } x \in \operatorname{dom} \gamma_i \\ \text{an arbitrary } a \in A_i \text{ otherwise.} \end{cases}$$

Let $\Phi \in \Gamma$. It is clear that

$$X_{\{\Phi\}} \subseteq \{i \mid \mathfrak{A}_i \models \Phi[\gamma i]\}.$$

Since $X_{\{\Phi\}} \in D$, we have $\{i \mid \mathfrak{A}_i \models \Phi[\gamma i]\} \in D$. By Theorem 1 $D\text{-prod}\,\mathfrak{A}_i \models \Phi[\gamma D]$. $\square$

Theorem 2 will be often used in the next chapters, especially in Chapter 5. Here we give a simple but sufficiently typical application of the theorem (see also Exercise 7).

COROLLARY 1. *If for any* $n \in \omega$ *a set of formulas* Γ *of a signature* Σ *has a model of power* $\geqslant n$, *then* Γ *has an infinite model.*

PROOF. We take an infinite set of symbols C for which $C \cap \cap (R \cup F) = \varnothing$ and let $\Sigma_1 = \langle R, F \cup C, \mu_1 \rangle$, where $\mu_1 \upharpoonright (R \cup \cup F) \approx \mu$ and $\mu_1(c) = 0$ for $c \in C$. Consider a set $X = \Gamma \cup \cup \{ \neg c \approx d \mid c, d \in C, c \neq d \}$ of sentences of a signature Σ_1. If $Y = \Gamma_1 \cup \{ \neg c_1 \approx d_1, \ldots, \neg c_n \approx d_n \}$, where $\Gamma_1 \subseteq \Gamma$ is a finite subset of X, then Y is satisfiable in a suitably expanded model $\mathfrak{A}$ of Γ of power $\geqslant n$. By the compactness theorem X has a model $\mathfrak{A}$. Since $\nu^{\mathfrak{A}}(c) \neq \nu^{\mathfrak{A}}(d)$ for $d, c \in C$, $c \neq d$, we conclude that $\mathfrak{A}$ is an infinite model of Γ. □

Since the set C in the proof of the corollary is arbitrary, we have in fact shown that under the hypothesis of Corollary 1 the set Γ has a model of a power exceeding any preassigned power.

Exercises

1. Show that a filtered product of partially ordered sets is a partially ordered set.

2. Show that the Cartesian product $K_1 \times K_2$ of two fields cannot be a field. (*Hint*. There are zero divisors in $K_1 \times K_2$.)

3. If all $\mathfrak{A}_i$, $i \in I$, are equal to a single system $\mathfrak{B}$, then the Cartesian (filtered) product I-prod $\mathfrak{A}$ (D-prod $\mathfrak{A}_i$) is said to be a Cartesian (filtered) power of $\mathfrak{B}$ and denoted by $\mathfrak{B}^I (\mathfrak{B}^D)$. Show that

(a) on all Cartesian powers $\mathfrak{B}^I$, with $|I| > 1$, the following formula is false:

$$\exists v_0 \exists v_1 (r(v_0) \wedge (r(v_1) \wedge (\neg v_0 \approx v_1 \wedge \forall v_2 (r(v_2) \to \\ \to (v_2 \approx v_0 \vee v_2 \approx v_1)))));$$

(b) a Cartesian power $\mathfrak{B}^I$, with carrier $\mathfrak{B}$ and set I having more than one element, cannot be a linearly ordered set.

4. Find nonisomorphic algebraic systems $\mathfrak{A}$ and $\mathfrak{B}$ for which the system $\mathfrak{A} \times \mathfrak{A}$ is isomorphic to $\mathfrak{B} \times \mathfrak{B}$. (*Hint*. Let $\Sigma = \langle r^1 \rangle$, $A = B = \omega$, $\nu^{\mathfrak{A}}(r) = \omega \setminus \{0\}$, $\nu^{\mathfrak{B}}(r) = \omega \setminus \{0, 1\}$.)

5. If $D_1 \subseteq D_2$ are two filters on a set I, then there is a homomorphism of a system D_1-prod $\mathfrak{B}_1$ onto D_2-prod $\mathfrak{B}_i$. (*Hint*. Consider a mapping assigning to an element $D_1 f$ an element $D_2 f$.)

6. Let D be a principal ultrafilter on I and $\cap D = \{ i_0 \}$. Then a system D-prod $\mathfrak{A}_i$ is isomorphic to the system $\mathfrak{A}_{i_0}$.

7. Let Γ be a set of sentences of a signature Σ such that for any algebraic system $\mathfrak{A}$ of Σ there is a sentence $\Phi \in \Gamma$ true on $\mathfrak{A}$. Show that there is a finite set $\{ \Phi_1, \ldots, \Phi_n \} \subseteq \Gamma$ such that the sentence $(\Phi_1 \vee (\Phi_2 \vee \ldots \vee \Phi_n)\ldots)$ is an identically true formula.

Chapter 4

THE CALCULUS OF PREDICATES

18. AXIOMS AND RULES OF INFERENCE

We fix some arbitrary signature Σ. In this section we define the *calculus of predicates* of Σ (abbreviated CP^{Σ}).

Formulas of CP^{Σ} are the formulas of Σ. *Sequents* of CP^{Σ} are sequences of the following four types:

$$\Phi_0, \ldots, \Phi_n \vdash \Psi; \quad \Phi_0, \ldots, \quad \Phi_n \vdash; \quad \vdash \Psi; \quad \vdash,$$

where $\Phi_0, \ldots, \Phi_n, \Psi$ are formulas of CP^{Σ}.

We adopt the following conventions. Let $x_1, \ldots, x_n$ be variables, let $t_1, \ldots, t_n$ be terms of Σ and let Φ be a formula of Σ. By $(\Phi)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ we denote the result of substituting terms $t_1, \ldots, t_n$ for all free occurrences in Φ of the variables $x_1, \ldots, x_n$ respectively. If there occurs $(\Phi)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ in the text, then it is assumed that for all $i = 1, \ldots, n$ none of the free occurrences in Φ of a variable x_i occurs in a subformula of Φ of the form $\forall y \Phi_1$ or $\exists y \Phi_1$ for $y \in \in FV(t_i)$. By $[\Phi]^x_y$ we denote a formula $(\Phi)^x_y$. Whenever $[\Phi]^x_y$ occurs it is in addition assumed that $y \notin FV(\Phi)$. If a notation $\Phi(x_1, \ldots, x_n)$ has already occurred in the text, instead of the cumbersome notation $(\Phi)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ we shall often write simply $\Phi(t_1, \ldots, t_n)$. Notice that by the convention at the beginning of Sec. 16 the variables $x_1, \ldots, x_n$ are pairwise distinct while there may be equal terms among $t_1, \ldots, t_n$.

DEFINITION. *Axioms* of CP^{Σ} are the following sequents:

(1) $\Phi \vdash \Phi$, with Φ a formula of CP^{Σ};

(2) $\vdash x \approx x$, with x a variable;

(3) $x \approx y, (\Phi)^z_x \vdash (\Phi)^z_y$, with x, y, z variables, Φ a formula of CP^{Σ} satisfying the condition on the notation $(\Phi)^z_x$ and $(\Phi)^z_y$.

DEFINITION. The rules of inference of CP^{Σ} are the following:

1. $\dfrac{\Gamma \vdash \Phi; \Gamma \vdash \Psi}{\Gamma \vdash \Phi \wedge \Psi}$; 2. $\dfrac{\Gamma \vdash \Phi \wedge \Psi}{\Gamma \vdash \Phi}$;

3. $\dfrac{\Gamma \vdash \Phi \wedge \Psi}{\Gamma \vdash \Psi}$;

4. $\dfrac{\Gamma \vdash \Phi}{\Gamma \vdash \Phi \vee \Psi}$;

5. $\dfrac{\Gamma \vdash \Psi}{\Gamma \vdash \Phi \vee \Psi}$;

6. $\dfrac{\Gamma, \Phi \vdash \mathrm{X};\ \Gamma, \Psi \vdash \mathrm{X};\ \Gamma \vdash \Phi \vee \Psi}{\Gamma \vdash \mathrm{X}}$;

7. $\dfrac{\Gamma, \Phi \vdash \Psi}{\Gamma \vdash \Phi \rightarrow \Psi}$;

8. $\dfrac{\Gamma \vdash \Phi;\ \Gamma \vdash \Phi \rightarrow \Psi}{\Gamma \vdash \Psi}$;

9. $\dfrac{\Gamma, \neg \Phi \vdash}{\Gamma \vdash \Phi}$;

10. $\dfrac{\Gamma \vdash \Phi;\ \Gamma \vdash \neg \Phi}{\Gamma \vdash}$;

11. $\dfrac{\Gamma, \Phi, \Psi, \Gamma_1 \vdash \mathrm{X}}{\Gamma, \Psi, \Phi, \Gamma_1 \vdash \mathrm{X}}$;

12. $\dfrac{\Gamma \vdash \Phi}{\Gamma, \Psi \vdash \Phi}$;

13. $\dfrac{\Gamma \vdash \Phi}{\Gamma \vdash \forall x \Phi}$, where x does not occur free in the elements of Γ;

14. $\dfrac{\Gamma, (\Phi)^x_t \vdash \Psi}{\Gamma, \forall x \Phi \vdash \Psi}$;

15. $\dfrac{\Gamma \vdash (\Phi)^x_t}{\Gamma \vdash \exists x \Phi}$;

16. $\dfrac{\Gamma, \Phi \vdash \Psi}{\Gamma, \exists x \Phi \vdash \Psi}$, where x does not occur free in Ψ and in the elements of Γ.

Just as in PC, in the rules of inference Φ, Ψ, X are variables for the formulas of CP and Γ, Γ_1 are variables for sequences of such formulas. In Rules 13 to 16 formulas Φ, Ψ and sequences Γ must satisfy the indicated conditions as well as the conditions on the notation $(\Phi)^x_t$. Just as in PC, if in the rules of inference the variables Φ, Ψ, Φ' and the variables Γ, Γ_1 are replaced by concrete formulas and concrete sequences of formulas, then instances (or applications) of the rules of inference result. If Θ is an instance of a rule of inference α, then we shall say that the sequent in Θ below the line is obtained from the sequents in Θ above the line with the aid of the rule α. The following definition is an almost word-for-word repetition of the corresponding definition of PC.

DEFINITION. A *linear proof* in CP^Σ is a finite sequence $C_0, \ldots, C_n$ of sequents of CP^Σ which satisfies the following condition: every sequent C_i, $i \leqslant n$, is either an axiom or is obtained from some preceding axioms using one of the rules of inference 1 to 16. A linear proof $C_0, \ldots, C_n$ is called a linear proof of its last sequent

C_n. If there is a linear proof in CP^Σ of a sequent C, then C is said to be CP^Σ-*provable* or a theorem of CP^Σ. A formula Φ of CP^Σ is said to be CP^Σ-provable or a theorem of CP^Σ if the sequent $\vdash \Phi$ is CP^Σ-provable. A tree D is said to be a *tree form proof* or a *proof tree of a sequent C in* CP^Σ if all of its initial sequents are axioms of CP^Σ, its passages are applications of Rules 1 to 16 and the final sequent is equal to C.

The definitions of an admissible rule and of a quasiderivation coincide with the corresponding definitions of Sec. 3, with PC replaced by CP^Σ.

PROPOSITION 1. *A sequent C is a theorem of* CP^Σ *if and only if there is a tree form proof of it in* CP.

PROOF. An almost word-for-word repetition of the proof of Proposition 3.1. □

A formula Ψ of CP^Σ is said to be a *tautology* if it is obtained from a formula Φ of the propositional calculus, provable in PC, by replacing all of its propositional variables by formulas of CP^Σ $\Psi_1, \ldots, \Psi_n$ respectively. The formula Φ is called the *base of the tautology*.

PROPOSITION 2. *Any tautology* Ψ *of* Σ *is* CP^Σ-*provable*.

PROOF. Let Ψ be obtained from a base Φ by replacing its variables $P_1, \ldots, P_n$ by formulas $\Psi_1, \ldots, \Psi_n$ respectively.

Let a tree D_1 be obtained from a proof tree D in PC of the sequent $\vdash \Phi$ by replacing the variables $P_1, \ldots, P_n$ by $\Psi_1, \ldots, \Psi_n$ respectively and by replacing the other propositional variables by an arbitrary formula Ψ_{n+1} of Σ. It is obvious that D_1 is a proof tree of the sequent $\vdash \Psi$ in CP^Σ. □

PROPOSITION 3. *If* Φ *is a formula of* CP^Σ, $x_1, \ldots, x_n$ *are variables,* $t_1, \ldots, t_n$ *are terms of* Σ *and the conditions of the notation* $(\Phi)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ *hold, then the following sequents are* CP^Σ-*provable*:

(a) $\forall x_1 \ldots \forall x_n \Phi \vdash (\Phi)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$;

(b) $(\Phi)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n} \vdash \exists x_1 \ldots \exists x_n \Phi$.

PROOF. Let $y_1, \ldots, y_n$ be pairwise distinct variables not occurring in Φ or $t_1, \ldots, t_n$ and different from $x_1, \ldots, x_n$.

(a) For all $1 < k < n$ we have an equation

$$\left(\forall x_{k+1} \ldots \forall x_n (\Phi)^{x_1, \ldots, x_{k-1}}_{y_1, \ldots, y_{k-1}}\right)^{x_k}_{y_k} = \forall x_{k+1} \ldots \forall x_n (\Phi)^{x_1, \ldots, x_k}_{y_1, \ldots, y_k}$$

and all the conditions on such a notation hold. Therefore the following tree is a proof in CP^{Σ}:

$$\begin{array}{c}
(\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n} \vdash (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n} \\ \hline
\forall x_n (\Phi)^{x_1,\ldots,x_n-1}_{y_1,\ldots,y_n-1} \vdash (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n} \\ \hline
\forall x_{n-1} \forall x_n (\Phi)^{x_1,\ldots,x_n-2}_{y_1,\ldots,y_n-2} \vdash (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n} \\
\vdots \qquad\qquad\qquad \vdots \\ \hline
\forall x_1 \ldots \forall x_n \Phi \vdash \Phi^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}
\end{array}$$

Applying now Rule 13 n times we obtain the provability in CP^{Σ} of the sequent

$$\forall x_1 \ldots \forall x_n \Phi \vdash \forall y_1 \ldots \forall y_n (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}.$$

We denote the formula $(\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}$ by Ψ. For Ψ then the condition on $(\Psi)^{y_1,\ldots,y_n}_{t_1,\ldots,t_n}$ holds. For all $1 < k < n$ we have

$$\left(\forall y_{k+1} \ldots \forall y_n (\Psi)^{y_1,\ldots,y_{k-1}}_{t_1,\ldots,t_{k-1}}\right)^{y_k}_{t_k} = \forall y_{k+1} \ldots \forall y_n (\Phi)^{y_1,\ldots,y_k}_{t_1,\ldots,t_k}$$

and conditions on such a notation. Applying again Rule 14 n times we obtain the provability in CP^{Σ} of the sequent

$$\forall y_1 \ldots \forall y_n \Psi \vdash (\Psi)^{y_1,\ldots,y_n}_{t_1,\ldots,t_n}.$$

Since $(\Psi)^{y_1,\ldots,y_n}_{t_1,\ldots,t_n} = (\Phi)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}$, the following tree is a quasi-derivation in CP^{Σ}:

$$\dfrac{\dfrac{\forall y_1 \ldots \forall y_n \Psi \vdash (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}}{\vdash \forall y_1 \ldots \forall y_n \Psi \to (\Phi)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}} ; \forall x_1 \ldots \forall x_n \Phi \vdash \forall y_1 \ldots \forall y_n \Psi}{\forall x_1 \ldots \forall x_n \Phi \vdash (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}}.$$

(b) The proof is similar to (a). Applying first Rule 15 several times we obtain the theorem

$$(\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n} \vdash \exists x_1 \ldots \exists x_n \Phi.$$

Applying then Rule 16 several times we obtain a theorem of CP^{Σ}

$$\exists y_1 \ldots \exists y_n (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n} \vdash \exists x_1 \ldots \exists x_n \Phi. \qquad (1)$$

Applying again Rule 15 several times we obtain the provability in CP^{Σ} of the sequent

$$(\Psi)^{y_1, \ldots, y_n}_{t_1, \ldots, t_n} \vdash \exists y_1 \ldots \exists y_n \Psi, \tag{2}$$

where $\Psi = (\Phi)^{x_1, \ldots, x_n}_{y_1, \ldots, y_n}$. From (1) and (2), just as in (a), we obtain the provability in CP^{Σ} of sequent (b). □

PROPOSITION 4. Admissible in CP^{Σ} are rules (a) to (l) of Proposition 3.2 and exercise 3.2, as well as the rule

$$\text{(m)} \quad \frac{\Phi_1, \ldots, \Phi_k \vdash \Psi}{(\Phi_1)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}, \ldots, (\Phi_k)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n} \vdash (\Psi)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}}.$$

PROOF. For rules (a) to (m) the proof essentially coincides with the proof of admissibility of the corresponding rules of Sec. 3.

(m) Let a sequent $\Phi_1, \ldots, \Phi_k \vdash \Psi$ be CP^{Σ}-provable. Applying Rule 7 several times we obtain the CP^{Σ} provability of the sequent

$$\vdash \Phi_1 \rightarrow (\Phi_2 \rightarrow \ldots (\Phi_k \rightarrow \Psi)\ldots).$$

Applying Rule 13 several times we obtain the provability of the sequent

$$\vdash \forall x_1 \ldots \forall x_n (\Phi_1 \rightarrow (\Phi_2 \rightarrow \ldots (\Phi_k \rightarrow \Psi)\ldots)).$$

From Proposition 3 (a) and admissible rule (e) we obtain the CP^{Σ}-provability of the sequent

$$\vdash (\Phi_1 \rightarrow (\Phi_2 \rightarrow \ldots (\Phi_k \rightarrow \Psi)\ldots))^{x_1, \ldots, x_n}_{t_1, \ldots, t_n} \tag{3}$$

From (3) and the axiom $(\Phi_1)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n} \vdash (\Phi_1)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ we obtain by Rules 8 and 12 the sequent

$$(\Phi_1)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n} \vdash (\Phi_2 \rightarrow (\ldots(\Phi_k \rightarrow \Psi)\ldots))^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}.$$

Similarly applying Rule 8 some more times we obtain the provability in CP^{Σ} of the sequent

$$(\Phi_1)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}, \ldots, (\Phi_k)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n} \vdash (\Psi)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}. \; \square$$

If C is a sequent of CP^{Σ}, then the union of all sets $FV(\Phi)$, where Φ is a formula in C, is said to be a set of free variables of C and denoted by $FV(C)$.

DEFINITION. Let C be a sequent of CP^Σ, $\mathfrak{A}$ an algebraic system of Σ and γ an interpretation of variables of $FV(C)$ in a set A. The sequent C is said to be *true in* $\mathfrak{A}$ *for the interpretation* γ (and we write $\mathfrak{A} \vDash C[\gamma]$) if and only if the following conditions hold:

(1) if $C = \Gamma \vdash \Psi$, then either $\mathfrak{A} \vDash \Psi[\gamma]$ or $\mathfrak{A} \vDash \neg\Phi[\gamma]$ for some formula Φ in Γ;

(2) if $C = \Gamma \vdash$, then $\mathfrak{A} \vDash \neg\Phi[\gamma]$ for some formula Φ in Γ; in particular, Γ is a nonempty sequence.

If the sequent C is not true in $\mathfrak{A}$ for γ, then we say that C is *false in* $\mathfrak{A}$ *for* γ. It follows from the definition that the sequent $\vdash$ is false on any algebraic system $\mathfrak{A}$..

DEFINITION. A sequent C of CP^Σ is said to be *identically true* if $\mathfrak{A} \vDash C[\gamma]$ for any algebraic system of Σ and any interpretation γ: $FV(C) \to A$.

It is clear that for a sequent C the property of being true is independent of what CP^Σ it is treated in (i. e. of Σ).

Our main aim in this chapter is to prove the following remarkable result due to K. Gödel: the class of CP^Σ-provable sequents coincides with the class of identically true sequents of CP^Σ. This statement is called the completeness theorem for the calculus of predicates. One part of it is easily proved.

THEOREM 1. *All* CP^Σ*-provable sequents* C *are identically true. In particular,* CP^Σ *is consistent, i. e. not all formulas of* CP^Σ *are* CP^Σ*-provable.*

PROOF. By induction on the height of the tree form proof of a sequent C. It is obvious that the axioms of CP^Σ are identically true. Verification that the Rules of inference 1 to 16 remain identically true will be left as an exercise to the reader. □

Notice only that to verify Rules 14, 15 we should first establish the following fact. Suppose that Φ is a formula, t is a term and the notation $(\Phi)^x_t$ has meaning. Let $X = FV(\Phi)$, $Y = FV((\Phi)^x_t)$, $\gamma: X \to A, \gamma^*: Y \to A$ and $\gamma \restriction (X \setminus \{x\}) = \gamma^* \restriction (Y \setminus \{x\})$. Then

$$\mathfrak{A} \vDash \Phi[\gamma] \Leftrightarrow \mathfrak{A} \vDash (\Phi)^x_t[\gamma^*],$$

if $x[\gamma] = t[\gamma^*]$. This fact is established by induction on the length of Φ. □

The second part of the completeness theorem is to be proved in Sec. 21. To do this we must first obtain a sufficient number of

CP^{Σ}-provable sequents. The following proposition shows that the ordinary properties of equality are CP^{Σ}-provable.

If $t_1, \ldots, t_n$, t the terms of Σ, $x_1, \ldots, x_n$, are variables, then $(t)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ denotes the result of substituting $t_1, \ldots, t_n$ for $x_1, \ldots, x_n$ respectively.

PROPOSITION 5. *If* $t, q, s; q_1, \ldots, q_n; s_1, \ldots, s_n$ *are terms of* Σ, Φ *is a formula of* CP^{Σ} *satisfying the conditions on* $(\Phi)^{x_1, \ldots, x_n}_{q_1, \ldots, q_n}$ *and on* $(\Phi)^{x_1, \ldots, x_n}_{s_1, \ldots, s_n}$, *then the following sequents are* CP^{Σ}*-provable*:

(a) $\vdash t \approx t$;

(b) $t \approx q \vdash q \approx t$;

(c) $t \approx q, q \approx s \vdash t \approx s$;

(d) $q_1 \approx s_1, \ldots, q_n \approx s_n \vdash (t)^{x_1, \ldots, x_n}_{q_1, \ldots, q_n} \approx (t)^{x_1, \ldots, x_n}_{s_1, \ldots, s_n}$;

(e) $q_1 \approx s_1, \ldots, q_n \approx s_n, (\Phi)^{x_1, \ldots, x_n}_{q_1, \ldots, q_n} \vdash (\Phi)^{x_1, \ldots, x_n}_{s_1, \ldots, s_n}$.

PROOF. (a) The sequent $\vdash t \approx t$ is obtained from the axiom $\vdash x \approx x$ by the derived rule (m) of Proposition 4.

Let x, x_1, y, z be pairwise distinct variables. Consider the tree

$$\begin{array}{c} \vdash x \approx x, x \approx y, (z \approx x)^{z}_{x} \vdash (z \approx x)^{z}_{y} \\ \hline x \approx y \vdash y \approx x \\ \hline t \approx q \vdash q \approx t \end{array}.$$

Since its initial sequents are axioms and its passages are applications of the rules of Proposition 4, the tree under consideration is a quasi-derivation of sequent (b). The provability of (c) is obtained in a similar way from the quasi-derivation

$$\begin{array}{c} y \approx z, (x \approx x_1)^{x_1}_{y} \vdash (x \approx x_1)^{x_1}_{z} \\ \hline x \approx y, y \approx z \vdash x \approx z \\ \hline t \approx q, q \approx s \vdash t \approx s \end{array}.$$

Let $y_1, \ldots, y_n; z_1, \ldots, z_n$ be pairwise distinct variables different from $x_1, \ldots, x_n$, not occurring in terms $q_1, \ldots, q_n, s_1, \ldots, s_n, t$ and in the formula Φ. From (a), Proposition 4(c) and from the fact that the terms $(t)^{x_1}_{y_1}$ and $\left((t)^{x_1}_{y_1}\right)^{z_1}_{y_1}$ are equal it follows that the tree

$$\begin{array}{c} \vdash (t)^{x_1}_{y_1} \approx (t)^{x_1}_{y_1};\ y_1 \approx z_1, (t)^{x_1}_{y_1} \approx \left((t)^{x_1}_{z_1}\right)^{z_1}_{y_1} \vdash (t)^{x_1}_{y_1} \approx (t)^{x_1}_{z_1} \\ \hline y_1 \approx z_1 \vdash (t)^{x_1}_{y_1} \approx (t)^{x_1}_{z_1} \end{array}$$

is a quasi-derivation in CP^{Σ}. If $n > 1$, then by Proposition 4(m) the sequent $y_1 \approx z_1 \vdash (t)^{x_1, x_2}_{y_1, y_2} \approx (t)^{x_1, x_2}_{z_1, y_2}$ is CP^{Σ}-provable. Applying to that sequent and to the axiom

$$y_2 \approx z_2, (t)^{x_1, x_2}_{y_1, y_2} \approx \left((t)^{x_1, x_2}_{z_1, z_2}\right)^{z_2}_{y_2} \vdash (t)^{x_1, x_2}_{y_1, y_2} \approx (t)^{x_1, x_2}_{z_1, z_2}.$$

Rule (4c) of Proposition 4 we obtain the sequent

$$y_1 \approx z_1, y_2 \approx z_2 \vdash (t)^{x_1, x_2}_{y_1, y_2} \approx (t)^{x_1, x_2}_{z_1, z_2}.$$

On carrying out a number of such steps we obtain the provability in CP^{Σ} of the sequent

$$y_1 \approx z_1, \ldots, y_n \approx z_n \vdash (t)^{x_1, \ldots, x_n}_{y_1, \ldots, y_n} \approx (t)^{x_1, \ldots, x_n}_{z_1, \ldots, z_n}.$$

From this we obtain by rule (m) of Proposition 4 sequent (d).

(e) Since an equation $\left((\Phi)^{x_1, x_2, \ldots, x_n}_{y_1, y_2, \ldots, y_n}\right)^{y_1}_{z_1} = (\Phi)^{x_1, x_2, \ldots, x_n}_{z_1, y_2, \ldots, y_n}$ is true, the sequent

$$y_1 \approx z_1, (\Phi)^{x_1, x_2, \ldots, x_n}_{y_1, y_2, \ldots, y_n} \vdash (\Phi)^{x_1, x_2, \ldots, x_n}_{z_1, y_2, \ldots, y_n}$$

is an axiom. If $n > 1$, then from this axiom and the axiom

$$y_2 \approx z_2, (\Phi)^{x_1, x_2, \ldots, x_n}_{z_1, y_2, \ldots, y_n} \vdash \left((\Phi)^{x_1, x_2, \ldots, x_n}_{z_1, y_2, \ldots, y_n}\right)^{y_2}_{z_2}$$

we obtain by Rule 4(e)

$$y_1 \approx z_1, y_2 \approx z_2, (\Phi)^{x_1, x_2, x_3, \ldots, x_n}_{y_1, y_2, y_3, \ldots, y_n} \vdash (\Phi)^{x_1, x_2, x_3, \ldots, x_n}_{z_1, z_2, y_3, \ldots, y_n}.$$

On carrying out a number of such steps we obtain the provability in CP^{Σ} of the sequent

$$y_1 \approx z_1, \ldots, y_n \approx z_n, (\Phi)^{x_1, \ldots, x_n}_{y_1, \ldots, y_n} \vdash (\Phi)^{x_1, \ldots, x_n}_{z_1, \ldots, z_n}.$$

From this by Proposition 4(m) we obtain the CP^{Σ} provability of sequent (e). □

The following theorem is, of course, a consequence of the Gödel theorem mentioned above, but it is also easy to prove directly.

THEOREM 2. *If* $\Sigma_1 \subseteq \Sigma$, *then* CP^{Σ} *is a conservative extension of* CP^{Σ_1}.

PROOF. Let D be a proof tree in CP^{Σ} of a sequent C which is also a sequent of CP^{Σ_1}. Let y be a variable occurring in none of the formulas of D. We define a mapping $\delta\colon T(\Sigma) \to T(\Sigma_1)$ by induction on the length of a term $t \in T(\Sigma)$:

(a) if t is a variable, then $\delta t = t$;

(b) if $t = f(t_1, \ldots, t_n)$, where f is a symbol in Σ_1, then $\delta t = f(\delta t_1, \ldots, \delta t_n)$;

(c) if $t = f(t_1, \ldots, t_n)$, where f is not a symbol in Σ_1, then $\delta t = y$.

If Φ is an atomic formula of Σ, then let $\delta\Phi$ be: (a) a formula $r(\delta t_1, \ldots, \delta t_n)$ if $\Phi = r(t_1, \ldots, t_n)$ and r is a symbol of Σ_1; (b) a formula $\delta t_1 \approx \delta t_2$ if $\Phi = t_1 \approx t_2$; (c) a formula $\forall y(y \approx y)$ if $\Phi = r(t_1, \ldots, t_n)$, where r is not a symbol of Σ_1. For any formula Φ of Σ we define a formula $\delta\Phi$ of Σ_1 to be a result of replacing in the formula Φ all atomic subformulas Ψ by $\delta\Psi$. Let δD be obtained from D by replacing all sequents $\Psi_1, \ldots, \Psi_n \vdash \Phi$ and $\Psi_1, \ldots, \Psi_n \vdash$ by $\delta\Psi_1, \ldots, \delta\Psi_n \vdash \delta\Psi$ and $\delta\Psi_1, \ldots, \delta\Psi_n \vdash$ respectively. It is obvious that the initial sequents of δD are axioms of CP^{Σ}. It is easy to verify that all passages in δD are applications of the same rules as the corresponding passages in D. Indeed, verification for Rules 1 to 13 and 16 is trivial, and for Rules 14 and 15 it is first necessary to notice by induction on the length of Φ (taking into account $x \neq y$) that $\delta(\Phi)^x_t = (\delta\Phi)^x_{\delta t}$ for which in turn it is necessary to establish by induction on the length of a term t_1 for any term t_2 the equation $\delta(t_1)^x_{t_2} = (\delta t_1)^x_{\delta t_2}$. Since $\delta\Phi = \Phi$ for all formulas Φ of a sequent C, δD is a proof of C in CP^{Σ_1}. □

In what follows we shall freely use Theorem 2 to avoid mentioning CP^{Σ} when the provability of some sequent C is discussed. In particular, we shall say that a sequent C is *provable in the calculus of predicates* or simply *provable* if C is provable in some CP^{Σ}.

Exercises

1. Let a signature Σ contain propositional variables of PC as 0-place predicate symbols. Show that CP^{Σ} is a conservative extension of PC. (*Hint*. Use the completeness theorem for PC and Theorem 1.)

2. Show that if in one of the Rules 13 to 16 we drop the restriction on the application of that rule (in particular, if for Rules 14 and 15 we drop the condition on

the notation $(\Phi)^x_t$), then a not identically true formula is provable in the calculus obtained.

3. Show that if in all of the Rules 13 to 16 we drop all the restrictions on the application of those rules, then all the theorems of the calculus J obtained will be 1-valid, and in particular J will be consistent.

19. THE EQUIVALENCE OF FORMULAS

All the properties of algebraic systems under study are invariant under an isomorphism; on the other hand, many properties of formulas of interest to us are invariant under the equivalence relation defined below.

We fix for further purposes an arbitrary signature Σ. In this section all formulas and algebraic systems have a signature Σ and proofs are considered in CP^{Σ}.

DEFINITION. Formulas Φ and Ψ are said to be *equivalent* (and we write $\Phi \equiv \Psi$) if two sequents, $\Phi \vdash \Psi$ and $\Psi \vdash \Phi$ are provable.

It is obvious that the relation $\equiv$ is an equivalence on the set $F(\Sigma)$ and that all provable formulas of $F(\Sigma)$ form one equivalence class. By Theorem 1, for any formulas $\Phi \equiv \Psi$, any system $\mathfrak{A}$ and any interpretation $\gamma\colon FV(\Phi) \cup FV(\Psi) \to A$ $\mathfrak{A} \vDash \Phi[\gamma]$ implies $\mathfrak{A} \vDash$ $\vDash \Psi[\gamma]$.

Notice that by Theorem 2 the relation $\Phi \equiv \Psi$ is independent of Σ.

DEFINITION. Formulas Φ and Ψ are said to be *propositionally equivalent* (and we write $\Phi \overset{s}{\equiv} \Psi$) if $\Phi \to \Psi$ and $\Psi \to \Phi$ are tautologies.

From Proposition 18.2 and Rule 8 we obtain

PROPOSITION 1. *Propositionally equivalent formulas Φ and Ψ are equivalent.* □

PROPOSITION 2. *If Φ, Ψ are formulas and x does not occur free in Ψ, then the following equivalences hold:*

(a) $\neg \exists x \Phi \equiv \forall x \neg \Phi$;
(b) $\neg \forall x \Phi \equiv \exists x \neg \Phi$;
(c) $\exists x \Phi \wedge \Psi \equiv \exists x (\Phi \wedge \Psi)$;
(d) $\forall x \Phi \wedge \Psi \equiv \forall x (\Phi \wedge \Psi)$;
(e) $\exists x \Phi \vee \Psi \equiv \exists x (\Phi \vee \Psi)$;

(f) $\forall x\,\Phi \vee \Psi \equiv \forall x\,(\Phi \vee \Psi)$;
(g) $\forall x\,\Phi \equiv \forall y[\Phi]^x_y$;
(h) $\exists x\,\Phi \equiv \exists y[\Phi]^x_y$.

PROOF. We give quasi-derivations for equivalences (a), (c), (e) and (g), leaving the verification of the rest to the reader.

(a)
$$\dfrac{\dfrac{\dfrac{\dfrac{\neg\Phi \vdash \neg\Phi}{\forall x\,\neg\Phi \vdash \neg\Phi}}{\Phi \vdash \neg\forall x\,\neg\Phi}}{\exists x\,\Phi \vdash \neg\forall x\,\neg\Phi}}{\forall x\,\neg\Phi \vdash \neg\exists x\,\Phi}, \qquad \dfrac{\dfrac{\dfrac{\dfrac{\Phi \vdash \Phi}{\Phi \vdash \exists x\,\Phi}}{\neg\exists x\,\Phi \vdash \neg\Phi}}{\neg\exists x\,\Phi \vdash \forall x\,\neg\Phi}}{\neg\forall x\,\Phi \vdash \exists x\,\neg\Phi}.$$

(c)
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Psi, \Phi \vdash \Phi \wedge \Psi}{\Psi, \Phi \vdash \exists x\,(\Phi \wedge \Psi)}}{\Psi, \exists x\,\Phi \vdash \exists x\,(\Phi \wedge \Psi)}}{\exists x\,\Phi \vdash \Psi \to \exists x\,(\Phi \wedge \Psi)}}{\vdash \exists x\,\Phi \to (\Psi \to \exists x\,(\Phi \wedge \Psi));\ \exists x\,\Phi \wedge \Psi \vdash \exists x\,\Phi}}{\exists x\,\Phi \wedge \Psi \vdash \Psi \to \exists x\,(\Phi \wedge \Psi); \qquad \exists x\,\Phi \wedge \Psi \vdash \Psi}}{\exists x\,\Phi \wedge \Psi \vdash \exists x\,(\Phi \wedge \Psi);},$$

$$\dfrac{\dfrac{\dfrac{\Phi \wedge \Psi \vdash \Phi}{\Phi \wedge \Psi \vdash \exists x\,\Phi};\ \Phi \wedge \Psi \vdash \Psi}{\Phi \wedge \Psi \vdash \exists x\,\Phi \wedge \Psi}}{\exists x\,(\Phi \wedge \Psi) \vdash \exists x\,\Phi \wedge \Psi}.$$

(e)
$$\dfrac{\exists x\,\Phi \vee \Psi \vdash \exists x\,\Phi \vee \Psi;\ \dfrac{\dfrac{\Phi \vdash \Phi \vee \Psi}{\Phi \vdash \exists x\,(\Phi \vee \Psi)}}{\exists x\,\Phi \vdash \exists x\,(\Phi \vee \Psi)};\ \dfrac{\Psi \vdash \Phi \vee \Psi}{\Psi \vdash \exists x\,(\Phi \vee \Psi)}}{\exists x\,\Phi \vee \Psi \vdash \exists x\,(\Phi \vee \Psi)};$$

$$\dfrac{\dfrac{\Phi \vee \Psi \vdash \Phi \vee \Psi;\ \dfrac{\dfrac{\Phi \vdash \Phi}{\Phi \vdash \exists x\,\Phi}}{\Phi \vdash \exists x\,\Phi \vee \Psi};\ \Psi \vdash \exists x\,\Phi \vee \Psi}{\Phi \vee \Psi \vdash \exists x\,\Phi \vee \Psi}}{\exists x\,(\Phi \vee \Psi) \vdash \exists x\,\Phi \vee \Psi}.$$

(g)
$$\dfrac{\dfrac{[\Phi]^x_y \vdash [\Phi]^x_y}{\forall x\,\Phi \vdash [\Phi]^x_y}}{\forall x\,\Phi \vdash \forall y\,[\Phi]^x_y}.$$

Before proving the last sequent notice that $\left[[\Phi]^x_y\right]^y_x = \Phi$. This equation follows from the conditions on the notation $[\Phi]^x_y$.

$$\cfrac{\cfrac{\left[[\Phi]^x_y\right]^y_x \vdash \Phi}{\forall y\, [\Phi]^x_y \vdash \Phi}}{\forall y\, [\Phi]^x_y \vdash \forall x\, \Phi}.\ \square$$

PROPOSITION 3. *All the equivalences of Secs.* 4, *and* 5 *hold if* Φ, *and* Ψ' *are assumed to be formulas of* Σ.

PROOF. Obvious since replacing the propositional variables by the formulas of CP^{Σ} changes the proofs in PC into the proofs in CP^{Σ}. □

THEOREM 3 (Replacement). *If a formula* Φ *is obtained from a formula* Ψ *of* Σ *by replacing some occurrence of a subformula* Ψ' *by a formula* Φ' *of* Σ *and* $\Phi' \equiv \Psi'$, *then* $\Phi \equiv \Psi$.

PROOF. By induction on the length of Ψ. If $\Psi' = \Psi$, then the statement is trivial. If $\Psi = \neg \Psi_1$ or $\Psi = \Psi_1 \tau \Psi_2$, where $\tau \in \{\wedge, \vee, \rightarrow\}$, then the proof of the induction step is similar to the corresponding cases of the replacement theorem for PC (Sec. 4). Thus to complete the proof it remains by the induction hypothesis to treat the cases where Ψ is of the form $\forall x \Psi'$ or $\exists x \Psi'$. Under the hypothesis the sequents $\Phi' \vdash \Psi'$ and $\Psi' \vdash \Phi'$ are provable. By virtue of the symmetry of Φ' and Ψ' it suffices to prove two sequents: $\forall x \Psi' \vdash \forall x \Phi'$ and $\exists x \Psi' \vdash \exists x \Phi'$. We give their quasi-derivations:

$$\cfrac{\cfrac{\Psi' \vdash \Phi'}{\forall x \Psi \vdash \Phi'}}{\forall x \Psi \vdash \forall x \Phi'}; \qquad \cfrac{\cfrac{\Psi' \vdash \Phi'}{\Psi' \vdash \exists x \Phi'}}{\exists x \Psi' \vdash \exists x \Phi'}.\ \square$$

In defining the truth of formulas on systems, bound occurrences of variables play an entirely different role from that of free occurrences. In particular, verification of the truth of the formulas $\forall x \Phi$ and $\forall y\, [\Phi]^x_y$ is the same. In the remainder of this section we show that replacing bound variables transforms a formula into an equivalent formula if under the transformation a new occurrence of the variable is bound by the same occurrence of the quantifier and no free occurrence of a variable becomes bound under such a replacement. We proceed to precise formulation of such a transformation.

DEFINITION. A formula Φ is said to be obtained from a formula Ψ by *replacing a bound variable* if Φ is obtained from Ψ by replacing some occurrence of a subformula $Qx\Psi_1$ by a formula $Qy[\Psi_1]_y^x$ (here $Q \in \{\forall, \exists\}$ and the conditions on the notation $[\Psi_1]_y^x$ hold). We say that formulas Φ and Ψ are *congruent* (and write $\Phi \sim \Psi$) if there is a sequence of formulas $\Phi_0, \ldots, \Phi_n$ such that $\Phi_0 = \Phi$, $\Phi_n = \Psi$ and Φ_{k+1}, $k < n$, is obtained from Φ_k by replacing a bound variable.

EXAMPLE. Consider formulas $\Phi = \forall\, v_2 \exists\, v_3 r(v_2, v_3)$ and $\Psi = \forall\, v_3 \exists\, v_2 r(v_3, v_2)$. The sequence

$$\forall\, v_2 \exists\, v_3 r(v_2, v_3), \qquad \forall\, v_2 \exists\, v_0 r(v_2, v_0),$$
$$\forall\, v_3 \exists\, v_0 r(v_3, v_0) \qquad \forall\, v_3 \exists\, v_2 r(v_3, v_2)$$

shows that $\Phi \sim \Psi$.

PROPOSITION 4. (a) *The relation* $\sim$ *is an equivalence on the set of formulas of* Σ.

(b) *If* $\Phi \sim \Psi$, *then* $\Phi \equiv \Psi$.

PROOF. (a) It follows from the property $\left[[\Psi_1]_y^x\right]_x^y = \Psi_1$ for any formula Ψ_1 for which the conditions on the notation $[\Psi_1]_y^x$ hold that if Ψ is obtained from Φ by replacing a bound variable, then Φ is also obtained from Ψ by replacing a bound variable. From this we obtain the symmetry of the relation $\sim$. The reflexivity and transitivity of the relation $\sim$ are obvious.

(b) By the replacement theorem it suffices to show that $Qx\Psi_1 \equiv Qy[\Psi_1]_y^x$, $Q \in \{\forall, \exists\}$. But this follows from Proposition 2 (n), (h). □

As already noted, we shall be interested in formulas mostly "up to" an equivalence, and so notation will be allowed of the form $\Phi_1 \wedge \ldots \wedge \Phi_n$, $\bigvee\limits_{k \leqslant n} \Phi_k$, etc. and others from which the formulas are ambiguously reconstructed but equivalent formulas are obtained with any bracket arrangements.

Exercises

1. Show that the relation $\equiv$ is an equivalence on $F(\Sigma)$.

2. Prove statements (b), (d), (f) and (h) of Proposition 2.

3. Show that for any formula Φ and any variables $x_1, \ldots, x_n$ there is a formula Ψ such that $\Psi \equiv \Phi$ and $\{x_1, \ldots, x_n\} \subseteq FV(\Psi)$.

20. NORMAL FORMS

Since we shall be concerned mostly with formulas "up to" an equivalence, it is useful to choose such subsets $P \subseteq F(\Sigma)$ of formulas that are constructed as far as possible more simply than arbitrary formulas and in such a way that for any $\Phi \in F(\Sigma)$ there is $\Psi \in P$ for which $\Phi \equiv \Psi$. Some of such subsets will be defined in this section.

We shall say that a formula Φ of Σ is in *disjunctive normal form* (abbreviated dnf) if it is obtained from a formula Ψ of the propositional calculus which is in dnf by replacing all propositional variables $P_1, \ldots, P_n$ occurring in Ψ by some atomic formulas $\Phi_1, \ldots, \Phi_n$ of Σ respectively.

DEFINITION. We shall say that a formula Φ of Σ is in *prenex normal form* if it has the form

$$Q_1 x_1 \ldots Q_n x_n \Phi_1,$$

where Q_i, $1 \leqslant i \leqslant n$, are quantifiers and Φ_1 is in dnf. In this case Φ_1 is called the *matrix* of the formula Φ and $Q_0 x_0, \ldots, Q_n x_n$ is its *quantifier prefix*.

THEOREM 4. *For any formula Φ of Σ there is a formula Ψ of Σ which is in prenex normal form and equivalent to Φ.*

PROOF. By Proposition 19.3 formulas $\Phi_1 \rightarrow \Phi_2$ and $\neg \Phi_1 \vee \Phi_2$ are equivalent for any $\Phi_1, \Phi_2 \in F(\Sigma)$. Hence for any $\Phi \in F(\Sigma)$ it is possible to obtain a formula $\Psi_1 \equiv \Phi$ containing no $\rightarrow$ sign by applying several times Theorem 3. We show by induction on the length of a formula Ψ_1 containing no $\rightarrow$ sign that there is $\Psi_2 \equiv \Psi_1$ of the form

$$Q_1 y_1 \ldots Q_k y_k \Psi_3,$$

where Ψ_3 is a quantifier-free formula, and the length of Ψ_2 is equal to the length of Ψ_1. If Ψ_1 is quantifier-free, then we take Ψ_1 as Ψ_2. If $\Psi_1 = Qx\Psi'$, then the required Ψ_2 exists by the induction hypothesis and Theorem 3. Thus it remains to consider the cases: (1) $\Psi_1 = \neg \Psi'$ and (2) $\Psi_1 = (\Psi' \tau \Psi'')$, $\tau \in \{\wedge, \vee\}$, where Ψ' has quantifiers and is in the form $Q_0 x_0 \ldots Q_n x_n \mathrm{X}$, where X is a quantifier-free formula. (Here we have used the equivalence $(\Psi' \tau \Psi'') \equiv (\Psi'' \tau \Psi')$ so as to state that Ψ' has quantifiers.) Let

$\Psi' = \exists x \Psi_4$. The case with the other quantifier is treated quite similarly. From Proposition 19.2(a) we obtain for case (1) an equivalence $\Psi_1 \equiv \forall x \neg \Psi_4$. The required Ψ_2 for case (1) then exists by the induction hypothesis and Theorem 3. Consider case (2). Let y be a variable not occurring in Ψ_1. From Proposition 19.2(h) and Theorem 3 we have $\Psi_1 \equiv (\exists y [\Psi_4]^x_y \tau \Psi'')$. From equivalences (c) and (e) of Proposition 19.2 we obtain $\Psi_1 \equiv$ $\equiv \exists y([\Psi_4]^x_y \tau \Psi'')$. The required Ψ_2 can now be found by the induction hypothesis and Theorem 3.

To complete the proof of the theorem, it is necessary by Theorem 3 to find $\Phi' \equiv \Psi_3$ in dnf for a quantifier-free Ψ_3. To do this we replace all atomic subformulas $\Phi_0, \ldots, \Phi_n$ of Ψ_3 by propositional variables $P_0, \ldots, P_n$ respectively and obtain a formula X of the propositional calculus. Let X_1 be a formula of the propositional calculus in dnf with the same variables as in X for which $X_1 \vdash X$ and $X \vdash X_1$ are theorems of PC. Let Φ' be obtained from X_1 by replacing $P_0, \ldots, P_n$ by $\Phi_0, \ldots, \Phi_n$ respectively. Then $\Phi' \overset{S}{\equiv} \Psi_3$ and so by Proposition 19.1 $\Phi' \equiv \Psi_3$. □

DEFINITION. We say that formula Φ of Σ is in *reduced normal form* if all of its atomic subformulas are atomical. (See Sec. 16 for the definition of an atomical formula.)

PROPOSITION 1. *For any formula Φ of Σ there is a formula Ψ of Σ in reduced normal form.*

PROOF. By Theorem 3 it suffices to prove the proposition for an atomic formula Φ. We proceed by induction on the number $n(\Phi)$ of occurrences of signature symbols in Φ. If $n(\Phi) \leqslant 1$, then Φ is an atomical formula and there is nothing to prove. If $n(\Phi) > 1$, then there is an occurrence of a term t of the form $f(v_{i_1}, \ldots, v_{i_k})$ in Φ. Hence $\Phi = (\Phi')^y_t$, where Φ' is obtained from Φ by replacing this occurrence by a variable y not occurring in Φ.

The following quasi-derivations:

$$\frac{\dfrac{\Phi \vdash \Phi;\ \vdash t \approx t}{\Phi \vdash (\Phi' \wedge y \approx t)^y_t}}{\Phi \vdash \exists y(\Phi' \wedge y \approx t)}; \qquad \frac{\dfrac{y \approx t,\ \Phi' \vdash \Phi}{\Phi' \wedge y \approx t \vdash \Phi}}{\exists y(\Phi' \wedge y \approx t) \vdash \Phi}$$

show that $\Phi \equiv \exists y(\Phi' \wedge y \approx t)$. Now we apply the induction hypothesis to Φ' and Theorem 3. □

Notice that in Theorem 4 it is possible to require without changing the proof that the formula Ψ should be in reduced normal form if Φ is in reduced normal form. Therefore we have

COROLLARY 1. *For any formula Φ of Σ there is a formula Ψ of Σ which is in prenex reduced normal form and is equivalent to Φ.* $\Box$

In what follows, instead of "prenex (reduced) normal form" we shall write "prenex (reduced) nf" for brevity.

Exercises

1. Show that in Theorem 4 it is possible to require that formulas Φ and Ψ should have the same number of occurrences of quantifiers.

2. Show that in Theorem 4 it is possible to require that Ψ should have the form:

$$\exists x_0 \forall x_1 \ldots \exists x_{n-1} \forall x_n \Psi'.$$

3. Verify that in Theorem 4 and Proposition 1 it is possible to require that $FV(\Phi) = FV(\Psi)$.

21. THEOREM ON THE EXISTENCE OF A MODEL

DEFINITION. A set of formulas X of Σ is said to be *inconsistent* or *incompatible* if in the calculus of predicates a sequent $\Gamma \vdash$, where all elements of Γ are in X, is provable. Otherwise X is *consistent* or *compatible.*

Note some simple properties of the notion.

PROPOSITION 1. (a) *An empty set is consistent.*

(b) *If X is a consistent set of formulas of Σ and in the calculus of predicates a sequent $\Phi_1, \ldots, \Phi_n \vdash \Phi$, where $\Phi \in F(\Sigma)$, $\Phi_0 \in X, \ldots, \Phi_n \in X$, is provable, then* X $\cup$ $\{\Phi\}$ *is consistent.*

(c) *If $X \cup \{\exists x \Phi\}$ is consistent, then $X \cup \{[\Phi]^x_y\}$ is consistent provided y does not occur free in the elements of X.*

(d) *If X_n, $n \in \omega$ are consistent sets and $X_n \subseteq X_{n+1}$, $n \in \omega$, then* $X = \bigcup\limits_{i \in \omega} X_n$ *is consistent.*

(e) *If X is a consistent set of formulas of Σ, then for any $\Phi \in F(\Sigma)$ either $X \cup \{\Phi\}$ or $X \cup \{\neg\Phi\}$ is consistent.*

PROOF. Statement (a) follows from Theorem 1. Statement (d) is obvious. If $\Phi_1, \ldots, \Phi_n \vdash \Phi$ is a theorem of the calculus of predicates, then the provability of the sequent $\Psi_1, \ldots, \Psi_k, \Phi \vdash$ implies that of $\Psi_1, \ldots, \Psi_k, \Phi_1, \ldots, \Phi_n \vdash$, so that (b) holds. If the sequent $\Phi_1, \ldots, \Phi_n, [\Phi]_y^x \vdash$ is provable in the calculus of predicates and y does not occur free in any of the formulas $\Phi_1, \ldots, \Phi_n$, then by the rule of Proposition 18.4(d) and Rule 13 we obtain the provability of $\Phi_1, \ldots, \Phi_n \vdash \forall y \neg [\Phi]_y^x$. Then it follows from Proposition 19.2(g) that a sequent $\Phi_1, \ldots, \Phi_n \vdash \forall x \neg \Phi$ is provable. From Proposition 19.2(a) it then follows that $\Phi_1, \ldots, \Phi_n \vdash$ $\vdash \neg \exists x \Phi$ is provable. Using now Rule 10 and the axiom $\exists x \Phi \vdash$ $\vdash \exists x \Phi$ we see that $\Phi_1, \ldots, \Phi_n, \exists x \Phi \vdash$ is a theorem of the calculus of predicates, whence we obtain (c). If $\Phi_1, \ldots, \Phi_n \Phi \vdash$ and $\Psi_1, \ldots, \Psi_k, \neg \Phi \vdash$ are theorems of the calculus of predicates, then by Rule 9, Proposition 18.4(d) and Rule 10 we obtain the provability of the sequent $\Phi_1, \ldots, \Phi_n, \Psi_1, \ldots, \Psi_k \vdash$, i. e. (e) holds. □

We now proceed to prove one of the most important theorems of mathematical logic.

THEOREM 5 (Existence of a Model). *Any consistent set X of formulas of Σ has a model.*

PROOF. By the compactness theorem (Sec. 17) it may be assumed that X is a finite set. Let $x_1, \ldots, x_n$ be all variables occurring free in the elements of $X = \{\Psi_1, \ldots, \Psi_k\}$. Since if X is satisfiable, $X' =$ $= \{\exists x_1 \ldots \exists x_n (\Psi_1 \wedge \ldots \wedge \Psi_k)\}$ is satisfiable, it may be assumed that X consists of a single sentence. Finally, $\Sigma = \langle R, F, \mu \rangle$ may be assumed to be finite. (If Σ is infinite, then it is necessary to take a restriction of Σ on the set of symbols occurring in the element X.)

Let $C = \{c_n \mid n \in \omega\}$ be a set of symbols, $c_n \neq c_k$ for $n \neq k$ and $C \cap (R \cup F) = \varnothing$. Let Σ_1 be obtained by adding to Σ the elements of C as symbols of new constants. Since formulas of Σ_1 are words of some countable alphabet, the set of all formulas of Σ_1 has a countable power. Let $\{\Phi_n \mid n \in \omega\}$ be the set of all sentences of Σ_1.

We construct a sequence

$$X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n \subseteq \ldots, \qquad n \in \omega,$$

of finite sets of sentences of Σ_1 as follows:

1. $X_0 = X$.
2. If $X_n \cup \{\Phi_n\}$ is inconsistent, then $X_{n+1} = X_n \cup \{\neg \Phi_n\}$.

3. If $X_n \cup \{\Phi_n\}$ is consistent and Φ_n does not begin with existential quantifier, then $X_{n+1} = X_n \cup \{\Phi_n\}$.

4. If $X_n \cup \{\Phi_n\}$ is consistent and $\Phi_n = \exists x \Phi'$, then $X_{n+1} = X_n \cup \{\Phi_n, (\Phi')^x_{c_k}\}$, where $c_k \in C$ is a constant with the least k, not occurring in Φ_n and the elements of X_n.

Set $X_\omega = \bigcup\limits_{n \in \omega} X_n$. We establish some properties of X_ω. Let Φ and Ψ be arbitrary sentences of Σ_1.

(a) X_ω is consistent;

(b) either $\Phi \in X_\omega$ or $\neg \Phi \in X_\omega$;

(c) if $\Phi_1, \ldots, \Phi_n \in X_\omega$ and $\Phi_1, \ldots, \Phi_n \vdash \Phi$ is provable, then $\Phi \in X_\omega$;

(d) $\Phi \wedge \Psi \in X_\omega \Leftrightarrow (\Phi \in X_\omega$ and $\Psi \in X_\omega)$;

(e) $\Phi \vee \Psi \in X_\omega \Leftrightarrow (\Phi \in X_\omega$ or $\Psi \in X_\omega)$;

(f) $\neg \Phi \in X_\omega \Leftrightarrow \Phi \notin X_\omega$;

(g) $\Phi \rightarrow \Psi \in X_\omega \Leftrightarrow (\Phi \notin X_\omega$ or $\Psi \in X_\omega)$;

(h) $\exists x \Phi \in X_\omega \Leftrightarrow ((\Phi)^x_c \in X_\omega$ for some $c \in C)$;

(i) $\forall x \Phi \in X_\omega \Leftrightarrow ((\Phi)^x_c \in X_\omega$ for any $c \in C)$;

(j) if t is a closed term of Σ_1 then $c \approx t \in X_\omega$ for some $c \in C$.

To prove (a) it suffices to establish by Proposition 1(d) that X_n, $n \in \omega$ are consistent. We proceed by induction on n. Under the hypothesis $X_0 = X$ is consistent. Let X_n be consistent. If for Φ_n Case 2 holds, then X_{n+1} is consistent by Proposition 1(e). In Case 3 X_{n+1} is consistent under the hypothesis. Let $X_n \cup \{\exists x \Phi'\}$ be consistent and suppose that D is a proof tree in CP^{Σ_1} of a sequent $\Psi_1, \ldots, \Psi_k, \exists x \Phi', [\Phi']^x_c \vdash$ where $c \in C$ does not occur in the formulas $\Psi_1, \ldots, \Psi_k, \exists x \Phi'$. Let y be a variable not occurring in D and D' be obtained from D by replacing all occurrences of c by y. It is obvious that D' will be a proof in CP^{Σ_1} of the sequent $\Psi_1, \ldots, \Psi_k, \exists x \Phi', [\Phi']^x_y \vdash$, which contradicts Proposition 1(c). Property (a) is thus proved. Property (b) follows immediately from the construction of X_ω, since $\Phi = \Phi_n$ for some $n \in \omega$. Property (c) follows easily from properties (a) and (b). Properties (d) to (g) follow easily from properties (a), (b) and (c). We prove property (h). Let $\Phi_n = \exists x \Phi$. If $\exists x \Phi \in X_\omega$, then by Property (a) $X_n \cup \{\Phi_n\}$ is consistent and so by construction $(\Phi)^x_c \in X_{n+1}$ for some $c \in C$. On the other hand, since $(\Phi)^x_c \vdash \exists x \Phi$ is a theorem of the calculus of predicates, it follows from $(\Phi)^x_c \in X_\omega$ and property (c) that $\exists x\Phi \in X_\omega$. We prove property (i). If $\forall x\Phi \in X_\omega$ and $c \in C$, then from the axiom $(\Phi)^x_c \vdash (\Phi)^x_c$ we obtain by Rule 14 a theorem $\forall x\Phi \vdash (\Phi)^x_c$. From this, by property (c) we obtain $(\Phi)^x_c \in X_\omega$. If $\forall x\Phi \notin X_\omega$, then by property (f) $\neg \forall x\Phi \in X_\omega$. From the equivalence $\neg \forall x\Phi \equiv \exists x \neg \Phi$ and (c) we obtain $\exists x \neg \Phi \in X_\omega$. By property (h) $(\neg \Phi)^x_c \in X_\omega$ for some $c \in C$. Then by property (f) $(\Phi)^x_c \notin X_\omega$. We now prove the last property, (j). By Proposition 18.5(a) $\vdash (x \approx y)^x_t$ is a theorem of the calculus of predicates. By Rule 15 $\vdash \exists x(x \approx t)$ is also a theorem. Now (j) follows from (c) and (h).

We define the relation $\sim$ on the set C as follows:

$$c \sim d \Leftrightarrow c \approx d \in X_\omega .$$

It follows from property (c) and Proposition 18.5 (a) to (c) that $\sim$ is an equivalence on C. If $c \in C$, then we denote by $\tilde{c}$ a $\sim$-equivalence class containing c. We proceed to define an algebraic system $\mathfrak{A} = \langle A, \nu^{\mathfrak{A}} \rangle$. Let $A = \{\tilde{c} \mid c \in C\}$. The signature of $\mathfrak{A}$ is $\Sigma_1 = \langle R, F \cup C, \mu_1 \rangle$. We define an interpretation $\nu^{\mathfrak{A}}$ of Σ_1 in A. Let $c, d_1, \dots, d_n \in C$. Then

(1) $\nu^{\mathfrak{A}}(c) = \tilde{c}$,

(2) $\langle \tilde{d}_1, \dots, \tilde{d}_n \rangle \in \nu^{\mathfrak{A}}(r) \Leftrightarrow r(d_1, \dots, d_n) \in X_\omega$, where $r \in R$, $\mu(r) = n$;

(3) if $f \in F$, $\mu(f) = n$, then $\nu^{\mathfrak{A}}(f)(\tilde{d}, \dots, \tilde{d}_n) = \tilde{c} \Leftrightarrow c \approx f(d_1, \dots, d_n) \in X_\omega$.

The correctness of defining the predicates of $\mathfrak{A}$ by point (2) follows from property (c) and Proposition 18.5(d). We verify that if $f \in F$, then point (3) is indeed a definition of an operation on A. Let $c \approx f(d_1, \dots, d_n) \in X_\omega$, $c' \approx f(e_1, \dots, e_n) \in X_\omega$ and $\tilde{d}_1 = \tilde{e}_1, \dots, \tilde{d}_n = \tilde{e}_n$. Then $d_1 \approx e_1 \in X_\omega, \dots, d_n \approx e_n \in X_\omega$, from which by property (c) and Proposition 18.5(d) $f(d_1, \dots, d_n) \approx f(e_1, \dots, e_n) \in X_\omega$ and hence, by property (c) and Proposition 18.5 (b) to (d), $c \approx c' \in X_\omega$, i. e. $\tilde{c} = \tilde{c}'$. On the other hand, for any $\tilde{d}_1, \dots, \tilde{d}_n \in A$ property (j) yields $c \approx f(d_1, \dots, d_n) \in X_\omega$ for some $c \in C$, i. e. $\nu^{\mathfrak{A}}(f)$ is defined at any $a_1, \dots, a_n \in A$.

We show by induction on the length of a closed term t of Σ_1 that

$$t^{\mathfrak{A}} = \tilde{c} \Leftrightarrow c \approx t \in X_\omega . \tag{1}$$

If t is a constant in C, then (1) follows from the definition of the relation $\sim$ and point (1) of the definition of $\nu^{\mathfrak{A}}$. For terms t of the form $f(d_1, \ldots, d_n)$, where $d_1, \ldots, d_n \in C$ and $f \in F$ (in particular, when t is a constant of Σ), equivalence (1) follows from point (3) of the definition of $\nu^{\mathfrak{A}}$. Let $t = f(t_1, \ldots, t_n), f \in F, \mu(f) = n \geqslant 1$ and $t_1^{\mathfrak{A}} = \tilde{d}_1, \ldots, t_n^{\mathfrak{A}} = \tilde{d}_n$. By the induction hypothesis $d_1 \approx t_1 \in \in X_\omega, \ldots, d_n \approx t_n \in X_\omega$ and so from Proposition 18.5 (d) and property (c) we get

$$f(t_1, \ldots, t_n) \approx f(d_1, \ldots, d_n) \in X_\omega. \tag{2}$$

By the definition of $\nu^{\mathfrak{A}}(f)$ we have

$$t^{\mathfrak{A}} = \tilde{c} \Leftrightarrow c \approx f(d_1, \ldots, d_n) \in X_\omega. \tag{3}$$

From (3), (2), Proposition 18.5 (b), (c) and property (c) we obtain (1).

By induction on the length of a sentence Φ of Σ_1 we show that

$$\mathfrak{A} \models \Phi \Leftrightarrow \Phi \in X_\omega. \tag{4}$$

If $\Phi = t_1 \approx t_2$, then according to (1) we have

$$\mathfrak{A} \models \Phi \Leftrightarrow (c \approx t_1 \in X_\omega, c \approx t_2 \in X_\omega \quad \text{for some } c \in C).$$

From this by Proposition 18.5 (b) to (d) and properties (c), (j) we obtain (4) for this case. Let $\Phi = r(t_1, \ldots, t_n)$, $r \in R$, and $t_1^{\mathfrak{A}} = = \tilde{d}_1, \ldots, t_n^{\mathfrak{A}} = \tilde{d}_n$. Using the definition of $\nu^{\mathfrak{A}}(r)$, (1), Proposition 18.5 and property (c) we obtain (4) for such Φ. For the remaining sentences Φ equivalence (4) follows immediately from the induction hypothesis and the corresponding properties (c) to (i).

Since $X \subseteq X_\omega$ it follows from (4) that $\mathfrak{A}$ is a model for a set X. □

A consequence of the above theorem is

THEOREM 6 (Gödel's Completeness Theorem). *If Φ is an identically true formula of the calculus of predicates, then Φ is provable in the calculus of predicates.*

PROOF. Since Φ is an identically true formula, it follows that the set $\{\neg\Phi\}$ has no model. From Theorem 5 we see that $\{\neg\Phi\}$ is inconsistent, i. e. $\neg\Phi\vdash$ is a theorem of the calculus of predicates. Using Rule 9 we conclude that Φ is provable. □

The proof of Theorem 5 gives us the following fact: a finite consistent set X of formulas of Σ has a finite or countable model

$\mathfrak{A}$. Unfortunately, the compactness theorem we have used for an arbitrary set X tells us nothing about the power of a model for X. However, the power of the method of proving Theorem 5 allows us to do without the compactness theorem and at the same time acquire information about the power of the model obtained. We first introduce one notion.

DEFINITION. A set of sentences X of Σ is said to be *complete* in Σ if X is consistent and for any sentence Φ of Σ either $\Phi \in X$ or $\neg \Phi \in \in X$.

PROPOSITION 2. *Any consistent set X of sentences of Σ is contained in some complete-in-Σ set of sentences Y.*

PROOF. Consider the family P of all consistent sets of sentences of Σ containing X. The inclusion relation $\subseteq$ partially-orders the set P. It is obvious that the union of any chain of $\langle P, \subseteq \rangle$ is in P. By the maximum principle $\langle P, \subseteq \rangle$ has a maximal element Y. It follows from Proposition 1 (e) that Y is a complete-in-Σ set. □

THEOREM 7. *If an infinite set X of formulas of Σ is consistent, then X has a model $\mathfrak{A}$ of a power not greater than that of X.*

PROOF. Let $FV(X)$ be all variables occurring free at least in one of the formulas of X. Consider a set $C' = \{c_x \mid x \in FV(X)\}$ of symbols such that $c_x \neq c_y$ for $x \neq y$ and $C' \cap (R \cup F) = \varnothing$. Let $\Sigma(X)$ be a signature all symbols of which occur at least in one of the formulas of X. Suppose that Σ_0 is obtained from $\Sigma(X)$ by adding elements of C' as symbols of new constants. By Corollary 13.1 $|\Sigma_0| \leqslant |X|$. Replace in all the formulas of X all free occurrences of the variables $x \in FV(X)$ by constants $c_x \in C'$ respectively. It is clear that the obtained set X' of sentences of Σ_0 has a model if and only if X has a model. The set X' is consistent *. Indeed, suppose that D is a proof tree of a sequent $(\Phi_1)^{x_1, \ldots, x_n}_{c_{x_1}, \ldots, c_{x_n}}, \ldots$ $\ldots, (\Phi_k)^{x_1, \ldots, x_n}_{c_{x_1}, \ldots, c_{x_n}} \vdash$, where $\Phi_1, \ldots, \Phi_k \in X$ and $c_{x_1}, \ldots, c_{x_n}$ are all constants of C' occurring in D. On replacing the constants $c_{x_1}, \ldots, c_{x_n}$ by variables $y_1, \ldots, y_n$ not occurring in D, we obtain a proof D' of the sequent $(\Phi_1)^{x_1, \ldots, x_n}_{y_1, \ldots, y_n}, \ldots, (\Phi_k)^{x_1, \ldots, x_n}_{y_1, \ldots, y_n} \vdash$. Applying Proposition 18.4 (g) (after first transposing one of the formulas to the right with a negation sign) we obtain the provability of $\Phi_1, \ldots$ $\ldots, \Phi_k \vdash$, which contradicts the compatibility of X.

---

* For reasons that are to become clear at the end of this section we are giving here a proof which is not based on Theorem 5.

We proceed to construct sets of sentences X_n, $n \in \omega$, and signatures Σ_n, $n \in \omega$. The following conditions will hold:

(1) $X_n \subseteq X_{n+1}$, $n \in \omega$, $X' \subseteq X_0$;

(2) X_n is a complete-in-Σ_n set of sentences;

(3) a signature Σ_{n+1} is obtained from Σ_n by adding new symbols of constants;

(4) $|\Sigma_n| \leqslant |X_n| = |X|$, $n \in \omega$.

As X_0 we take a complete-in-Σ_0 set of sentences, containing X'. If X_n is already constructed, then Σ_{n+1} is obtained from Σ_n by adding a set $\{c^n_\Phi \mid \Phi \in X_n\}$ of new symbols of constants. Consider a set of sentences

$$X'_n = X_n \cup \left\{(\Phi)^x_{c^n_\Psi} \,\middle|\, \Psi = \exists x\Phi,\ \Psi \in X_n\right\}$$

of Σ_{n+1}. The set X'_n is consistent. Indeed, suppose that for $\{\Psi'_1, \ldots, \Psi'_k, \Psi_1, \ldots, \Psi_m\} \subseteq X_n$, $\Psi_1 = \exists z_1 \Phi_1, \ldots, \Psi_m = \exists z_m \Phi_m$ the sequent

$$\Psi'_1, \ldots, \Psi'_k,\quad (\Phi_1)^{z_1}_{c^n_{\Psi_1}}, \ldots, (\Phi_m)^{z_m}_{c^n_{\Psi_m}} \vdash$$

is provable and m is such a minimal number. On replacing in the proof D of this sequent the constant $c^n_{\Psi_1}$ by a variable y not occurring in D we obtain a proof D' of a sequent

$$\Psi'_1, \ldots, \Psi'_k, [\Phi_1]^{z_1}_y,\quad (\Phi_2)^{z_2}_{c^n_{\Psi_2}}, \ldots, (\Phi_m)^{z_m}_{c^n_{\Psi_m}} \vdash .$$

It follows from Proposition 1 (c) that the sequent

$$\Psi'_1, \ldots, \Psi'_k, \exists z_1 \Phi_1, (\Phi_2)^{z_2}_{c^n_{\Psi_2}}, \ldots, (\Phi_m)^{z_m}_{c^n_{\Psi_m}} \vdash$$

is provable, which contradicts the minimality of m. As X_{n+1} we now take a complete-in-Σ_{n+1} set of sentences, containing X'_n. Let $X_\omega = \bigcup_{n \in \omega} X_n$ and let C be the set of all constants of all Σ_n, $n \in \omega$. Since every X_n is consistent, so is X_ω. It is also obvious that X_ω is a complete-in-Σ_ω set, where $\Sigma_\omega = \bigcup_{n \in \omega} \Sigma_n$ is obtained from Σ by adding elements of C as symbols of constants. Hence X_ω has properties (a) and (b) of the proof of Theorem 5, where Σ_ω is considered instead of Σ_1. If properties (a) and (b) hold, then properties (c) to

(g) hold. Property (h) follows from the construction of sets X'_n, $n \in \omega$. Finally, properties (i), (j) follow from property (h) just as in Theorem 5. It is then necessary to repeat the end of the proof of Theorem 5 beginning with the definition of the relation $\sim$ on C.

It remains only to notice that the power of a model $\mathfrak{A}$ is not greater than that of the set C which in turn is the union of a countable number of sets with a power not greater than that of X and hence has a power not greater than that of $\omega \times X$. By Corollary 13.1(a) we have $|\omega \times X| = |X|$. □

Theorem 7 together with Theorem 1 gives also a new proof of the compactness theorem. (See the footnote on page 137).

Exercises

1. Give an example of a formula Φ of the calculus of predicates for which the sets $\{\Phi\}$ and $\{\neg\Phi\}$ are consistent.
2. Derive the compactness theorem from Theorems 1 and 7.
3. From Theorems 1 and 6, obtain a characterization of provable sequents of CP^{Σ}: a sequent C of CP is CP^{Σ}-provable if and only if C is identically true.

22. HILBERTIAN CALCULUS OF PREDICATES

We fix an arbitrary signature Σ. All signature-dependent notions of this section will relate to Σ.

In this section we treat CP_1^{Σ} called the *Hilbertian calculus of predicates* and show its equivalence in a certain sense (Theorem 9) to CP^{Σ}, just as the equivalence of PC and PC_1 was shown in Sec. 8.

The definition of a *formula* of CP_1^{Σ} is the same as that for CP^{Σ}. There are no sequents in CP_1^{Σ}.

The *axioms* of CP_1^{Σ} are obtained from the following fourteen schemata by replacing the variables Φ, Ψ, X by concrete formulas of CP_1^{Σ}; x, y, z are variables and t are terms of CP_1^{Σ}:

1. $\Phi \to (\Psi \to \Phi)$,
2. $(\Phi \to \Psi) \to ((\Phi \to (\Psi \to X)) \to (\Phi \to X))$,
3. $(\Phi \wedge \Psi) \to \Phi$,
4. $(\Phi \wedge \Psi) \to \Psi$,
5. $(\Phi \to \Psi) \to ((\Phi \to X) \to (\Phi \to (\Psi \wedge X)))$,

6. $\Phi \to (\Phi \vee \Psi)$,
7. $\Phi \to (\Psi \vee \Phi)$,
8. $(\Phi \to \mathrm{X}) \to ((\Psi \to \mathrm{X}) \to ((\Phi \vee \Psi) \to \mathrm{X}))$,
9. $(\Phi \to \Psi) \to ((\Phi \to \neg \Psi) \to \neg \Phi)$,
10. $\neg \neg \Phi \to \Phi$,
11. $\forall x \Phi \to (\Phi)_t^x$,
12. $(\Phi)_t^x \to \exists x \Phi$,
13. $x \approx x$,
14. $x \approx y \to ((\Phi)_x^z \to (\Phi)_y^z)$.

The *rules of inference* of CP_1^Σ are:

1. $\dfrac{\Phi, \Phi \to \Psi}{\Psi}$,

2. $\dfrac{\Psi \to \Phi}{\Psi \to \forall x \Phi}$,

3. $\dfrac{\Phi \to \Psi}{\exists x \Phi \to \Psi}$,

where x does not occur free in Ψ in Rules 2 and 3.

A *proof* in CP_1^Σ of a formula Φ is a sequence $\Phi_0, \ldots, \Phi_n$ of formulas of CP_1^Σ such that $\Phi_n = \Phi$ and for every $i \leqslant n$ Φ_i satisfies one of the following conditions:

(1) Φ_i is an axiom of CP_1^Σ,

(2) Φ_i is obtained from some Φ_j, $j < i$, by one of the Rules 1 to 3.

If there is a proof in CP_1^Σ of a formula Φ, then Φ is said to be CP_1^Σ*-provable* or a *theorem* in PC_1^Σ (and we write $\rhd \Phi$).

A *derivation in* CP_1^Σ *of a formula* Φ *from a set of formulas* G is a sequence $\Phi_0, \ldots, \Phi_n$ of formulas of CP_1^Σ such that $\Phi_n = \Phi$ and for every $i \leqslant n$ a formula Φ_i satisfies one of the following conditions:

(1) Φ_i is provable in CP_1^Σ,

(2) Φ_i is in G,

(3) Φ_i is obtained from some Φ_j, $j < i$, by one of the Rules 1 to 3. The variable x must not occur free in any of the formulas of G when Rules 2 and 3 are applied.

If there is a derivation in CP_1^Σ of a formula Φ of G, then Φ is said to be CP_1^Σ*-derivable from* G. G is then called a set of hypotheses. It is obvious that the derivability of a formula is equivalent to its derivability from an empty set of hypotheses. Therefore the derivability of Φ from G may be denoted by $G \rhd \Phi$. In this section, unless otherwise stated, by proof and derivation we mean proof and derivation in CP_1^Σ.

The rule of inference

$$\frac{\Psi_1, \ldots, \Psi_k}{\Phi}$$

is said to be CP_1^Σ*-admissible* if adding it to CP_1^Σ does not affect the set of provable formulas.

PROPOSITION 1. *The following rules are* CP_1^Σ*-admissible*:

$$\text{(a)}\ \frac{\Phi}{\forall x\, \Phi}\ ; \quad \text{(b)}\ \frac{(\Phi)_t^x}{\exists x\, \Phi}\ ; \quad \text{(c)}\ \frac{(\Phi)_t^x \to \Psi}{\forall x\, \Phi \to \Psi}\ ; \quad \text{(d)}\ \frac{\Psi \to (\Phi)_t^x}{\Psi \to \exists x\, \Phi}\ .$$

PROOF. (a) Let Ψ be some provable sentence. Then by Axiom 1, the provability of Φ and Rule 1 we get $\rhd \Psi \to \Phi$. By Rule 2 we get $\rhd \Psi \to \forall x \Phi$. From this the provability of $\forall x \Phi$ follows by Rule 1.

(c) The formula $\forall x \Phi \to \Psi$ is obtained from the axiom $\forall x \Phi \to (\Phi)_t^x$ and the theorem $(\Phi)_t^x \to \Psi$ with the aid of Axioms 1, 2 and Rule 1.

The proof of statements (b) and (d) will be left to the reader (Exercise 1). □

Formulas Φ and Ψ are said to be *equivalent in* CP_1^Σ if provable in CP_1^Σ are the formulas $\Phi \to \Psi$ and $\Psi \to \Phi$ (this is denoted by $\Phi \overset{1}{\equiv} \Psi$).

PROPOSITION 2. *Any tautology* Φ *is* CP_1^Σ*-provable.*

PROOF. Let Ψ be a base of Φ. By Theorem 8.11 Ψ is CP_1-provable. It is clear that on replacing the propositional variables in the proof in PC_1 of the formula Ψ by the corresponding formulas of CP_1^Σ we obtain a proof of Φ in CP_1^Σ. □

COROLLARY 1. *If* Φ *and* Ψ *are propositionally equivalent formulas* of CP_1^Σ, *then the* CP_1^Σ *provability of* Φ *is equivalent to the* CP_1^Σ *provability of* Ψ. □

THEOREM 8. (Deduction). *If* $G \cup \{\Phi, \Psi\}$ *is a set of formulas of* CP_1^Σ *then* $G \cup \{\Phi\} \rhd \Psi$ *implies* $G \rhd \Phi \to \Psi$.

PROOF. By induction on the length n of a minimal derivation $\Psi_1, \ldots, \Psi_n$ of Ψ from $G \cup \{\Phi\}$. The case where $n = 1$ (i. e. Ψ is a theorem of CP_1^Σ or is in $G \cup \{\Phi\}$) as well as the case where Ψ_n is obtained by Rule 1 are quite similar to the corresponding cases for PC_1 and have already been treated in the proof of Theorem 8.12. Since the derivation is minimal, it remains to treat the cases where Ψ is obtained from Ψ_{n-1} by Rule 2 or 3. By the induction hypothesis we already have $G \rhd \Phi \to \Psi_{n-1}$.

Let $\Psi_{n-1} = (\Theta_1 \to \Theta_2)$ and $\Psi = (\Theta_1 \to \forall x\, \Theta_2)$. By the definition of derivation, x does not occur free in Φ, the elements of G and Θ_1. Since $\Phi \to (\mathrm{X}_1 \to \mathrm{X}_2)$ and $(\Phi \wedge \mathrm{X}_1) \to \mathrm{X}_2$ are propositionally equivalent for any formulas X_1, X_2, by Corollary 1 the sequence

$$\Phi \to \Psi_{n-1},\ (\Phi \wedge \Theta_1) \to \Theta_2,\ (\Phi \wedge \Theta_1) \to \forall x\Theta_2,\ \Phi \to (\Theta_1 \to \forall x\Theta_2)$$

can be supplemented to a derivation of $\Phi \to \Psi$ from G.

Now let Ψ be obtained by Rule 3. Then $\Psi_{n-1} = (\Theta_1 \to \Theta_2)$ and $\Psi = (\exists x\Theta_1 \to \Theta_2)$. Here x does not occur free in Φ, Θ_2 and the elements of G. By virtue of the propositional equivalences

$$\Phi \to \Psi_{n-1} \overset{s}{\equiv} \Theta_1 \to (\Phi \to \Theta_2) \quad \text{and} \quad \exists x\Theta_1 \to (\Phi \to \Theta_2) \overset{s}{\equiv} \Phi \to (\exists x\Theta_1 \to \Theta_2)$$

the following sequence

$$\Phi \to \Psi_{n-1},\ \Theta_1 \to (\Phi \to \Theta_2),\ \exists x\Theta_1 \to (\Phi \to \Theta_2),\ \Phi \to (\exists x\Theta_1 \to \Theta_2)$$

can be supplemented to a derivation of $\Phi \to \Psi$ from G. □

COROLLARY 2. *Let* $\Phi_1, \ldots, \Phi_n$, Φ *be formulas of* CP_1^Σ. *Then* $\{\Phi_1, \ldots, \Phi_n\} \rhd \Phi$ *is equivalent to* $\rhd\ \Phi_1 \to (\Phi_2 \to \ldots (\Phi_n \to \Phi)\ldots)$, *which in turn is equivalent to* $\rhd\ (\Phi_1 \wedge (\ldots(\Phi_{n-1} \wedge \Phi_n)\ldots)) \to \Phi$.

PROOF. For the first of the equivalences we apply n times Theorem 8 and Rule 1. For the second the same reasoning is applied as that in Corollary 8.1. □

THEOREM 9. *For a formula* Φ *to be* CP_1^Σ*-derivable from the set of all terms of a finite sequence of formulas* Γ *it is necessary and sufficient that the sequent* $\Gamma \vdash \Phi$ *be* CP^Σ*-provable. In particular, the sets of* CP_1^Σ*- and* CP^Σ*-provable formulas coincide.*

PROOF. By Rules 7 and 8 of CP^Σ a sequent $\Psi_1, \ldots, \Psi_n \vdash \Phi$ is CP^Σ-provable if and only if so is $\vdash \Psi_1 \to (\Psi_2 \to \ldots (\Psi_n \to \Phi)\ldots)$.

Then it follows from Corollary 2 that to prove necessity it is possible to restrict one's attention to the case $\Gamma = \varnothing$. It is easily verified that the axioms of CP_1^Σ are identically true and that the rules of inference of CP_1^Σ remain identically true. Therefore necessity follows from Gödel's completeness theorem.

Sufficiency. It is obvious that if $\Gamma \vdash \Phi$ is an axiom of CP^Σ, then $\Gamma \rhd \Phi$. (Here and on we allow some abuse in notation: we should write $\{\Psi_1, \ldots, \Psi_n\} \rhd \Phi$ if $\Gamma = \langle \Psi_1, \ldots, \Psi_n \rangle$.) Let Φ_0 be some sentence of Σ. Since the rules

$$\frac{\Gamma \vdash}{\Gamma \vdash \Phi_0 \wedge \neg \Phi_0}, \qquad \frac{\Gamma \vdash \Phi_0 \wedge \neg \Phi_0}{\Gamma \vdash}$$

are CP^Σ-admissible, it remains to show that if in the rules of inference of CP^Σ we replace the $\vdash$ sign by $\rhd$ and $\Gamma \vdash$ by $\Gamma \rhd \Phi_0 \wedge \neg \Phi_0$, then the truth of the statement above the line will imply the truth of the statement below the line. For Rules 1 to 12 verification is the same as in Theorem 8.11. For Rules 13 and 15, when $\Gamma = \varnothing$ this is true by virtue of Proposition 1(a), (b). For the remaining cases this follows from Corollary 2, Rules 2, 3 of CP_1^Σ and Proposition 1(c), (d). □

From the theorem above and Theorem 2 we obtain

COROLLARY 3. *If* $\Sigma_1 \subseteq \Sigma$, *then* CP_1^Σ *is a conservative extension of* $\mathrm{CP}_1^{\Sigma_1}$. □

From Theorem 9 it also follows that $\Phi \stackrel{1}{=} \Psi$ is equivalent to $\Phi \equiv \Psi$.

COROLLARY 4. *Let* $X \cup \{\Phi\}$ *be a set of formulas of* Σ *and let* Y *be the set of all variables occurring free at least in one of the formulas of* $X \cup \{\Phi\}$. *For* $X \rhd \Phi$ *to hold it is necessary and sufficient that the following condition hold: for any algebraic system* $\mathfrak{A}$ *of* Σ *and any interpretation* $\gamma\colon Y \to A$, *if* $\mathfrak{A} \models \Psi[\gamma]$ *holds for any* $\Psi \in X$, then $\mathfrak{A} \models \Phi[\gamma]$.

PROOF. Since a derivation contains only a finite set of formulas, $X \rhd \Phi$ is the same as $X_1 \rhd \Phi$ for some finite $X_1 \subseteq X$. Necessity then follows from Theorems 1 and 9. If $\mathfrak{A} \models \Psi[\gamma]$, $\Psi \in X$ implies $\mathfrak{A} \models \Phi[\gamma]$ for any systems $\mathfrak{A}$ of Σ and $\gamma\colon Y \to A$, then the set $X \cup \{\neg\Phi\}$ has no model. Hence by Theorem 5 a sequent $\Psi_1, \ldots, \Psi_n \vdash \Phi$ is provable for some $\Psi_1, \ldots, \Psi_n \in X$ and sufficiency is obtained from Theorem 9. □

Exercises

1. Prove statements (b) and (d) of Proposition 1.

2. Prove that $\Gamma \rhd \Phi$ if and only if there is a sequence $\Phi_0, \ldots, \Phi_n$ of formulas of CP_1^Σ such that $\Phi_n = \Phi$ and for every $i \leqslant n$ the formula Φ_i satisfies one of the following conditions:

(1) Φ_i is CP_1^Σ-provable,

(2) Φ_i is in Γ,

(3) Φ_i is obtained from some Φ_j, $j < i$, by Rule 1.

23. PURE CALCULUS OF PREDICATES

In this section we define what is known as the *pure calculus of predicates* (abbreviated CPP) and prove some "universality" of the calculus (Theorem 11).

Consider a signature $\Sigma^* = \langle R^*, F^*, \mu^* \rangle$ having the following properties:

(1) $F^* = \varnothing$, $R^* = \{ r_m^k \mid k, m \in \omega \}$;

(2) $\mu^*(r_m^k) = k$ for any $m \in \omega$ and $k \in \omega$.

Formulas of CPP are formulas of Σ^* containing no symbol of equality. *Sequents* of CPP are sequents of CP^{Σ^*} in which all formulas are formulas of CPP.

Axioms of CPP are only sequents of the form $\Phi \vdash \Phi$; the *rules of inference* are the same as in CP^{Σ^*}. A proof in CPP is defined in the same way as in CPP^{Σ^*}, now understanding by formulas, sequents and axioms, of course, those of CPP. It is easy to verify that all the results of Sec. 18 to 20 relating to CP^{Σ^*}, except for Proposition 18.5 and Theorem 2, also hold for CPP, since axioms (2) and (3) are not used in their proofs. Now we show that the results of Sec. 21 also carry over to CPP. In fact we have

THEOREM 10. CP^{Σ^*} *is a conservative extension of CPP.*

PROOF. A set X of sentences of CPP is said to be compatible in CPP if for any $\Phi_1, \ldots, \Phi_n \in X$ the sequent $\Phi_1, \ldots, \Phi_n \vdash$ is not CPP-provable. We show that any CPP-compatible set of formulas of CPP has a model. The proof of this statement differs but little from that of Theorem 5. The construction of the set X_ω is the same. (By formulas and proofs, of course, we understand here formulas and proofs in CPP. The proofs of properties (a) to (i) for X_ω are the same. Property (j) is not required in this case. The relation $\sim$ on C is not defined and the carrier of a system $\mathfrak{A}$ is the set C itself. To prove the equivalence

$$\mathfrak{A} \models \Phi(d_1, \dots, d_n) \Leftrightarrow \Phi(d_1, \dots, d_n) \in X_\omega$$

from properties (a) to (i) is still simpler than in Theorem 5, since there is no need to change to the representatives of $\sim$-equivalence classes and there are no atomic formulas of the form $t_1 \approx t_2$.

If now $S = \Psi_1, \dots, \Psi_n \vdash \Phi$ is a theorem of CP^{Σ^*} which is a sequent of CPP, then by Theorem 1, S is an identically true sequent. Therefore by what has just been proved $\{\Psi_1, \dots, \Psi_n, \neg\Phi\}$ is not a CPP-compatible set and so the sequent $\Psi_1, \dots, \Psi_n, \neg\Phi \vdash$ is CPP-provable. By Rule 9 we obtain the CPP provability of S. If $S = \Psi_1, \dots, \Psi_n \vdash$, then $\{\Psi_1, \dots, \Psi_n\}$ is not a CPP-compatible set and so again $\Psi_1, \dots, \Psi_n \vdash$ is a theorem of CPP. □

It is clear that from the results of Sec. 21 and Theorem 10 we obtain the validity of all the theorems obtained from the theorems of Sec. 21 by replacing CP^Σ by CPP. The end of this section will be devoted to a fact that shows that questions of provability in various CP^Σ's "reduce" to questions of provability in CPP. We proceed to precise formulations.

We fix a predicate symbol $r_0 \in R^*$ for which $\mu_0(r_0) = 2$.

DEFINITION. Let $\Sigma = \langle R, F, \mu\rangle$ be a finite or countable signature. A distinct-valued mapping $\alpha\colon R \cup F \to R^*$ is said to be an interpretation of Σ in Σ^* if the following conditions hold: (a) $r_0 \notin \alpha(R \cup F)$; (b) if $s \in R$, then $\mu^*(\alpha s) = \mu(s)$; (c) if $f \in F$, then $\mu^*(\alpha f) = \mu(f) + 1$. For an interpretation α of Σ in Σ^* we define a mapping α^* of the set of formulas of Σ in reduced normal form into a set of formulas of CPP by induction. If Φ is an atomical formula of the form $x \approx y$, then $\alpha^*(\Phi) = r_0(x, y)$; if Φ is an atomical formula of the form $s(x_1, \dots, x_n)$, then $\alpha^*\Phi = \alpha s(x_1, \dots, x_n)$; if Φ is an atomical formula of the form $y \approx f(x_1, \dots, x_n)$ or $f(x_1, \dots, x_n) \approx y$, then $\alpha^*\Phi = \alpha f(x_1, \dots, x_n, y)$; if $\Phi = \neg\Psi$, $\Phi = Qx\Psi$ or $\Phi = \Psi_1 \tau \Psi_2$, where $Q \in \{\forall, \exists\}$, $\tau \in \{\wedge, \vee, \to\}$, then $\alpha^*\Phi$ is equal to $\neg\alpha^*\Psi$, $Qx\alpha^*\Psi$ or $\alpha^*\Psi_1\tau\alpha^*\Psi_2$ respectively. If α is an interpretation of Σ in Σ^*, $\Phi \in F(\Sigma)$ is in reduced nf and $\Sigma(\Phi) = \langle\{s_0, \dots, s_k\}, \{f_0, \dots, f_m\}, \mu'\rangle$, then by $\alpha_0\Phi$ we denote the conjunction of the following sentences of Σ_0 (where $n_j = \mu'(s_j)$, $l_i = \mu'(f_i)$, $x, y, z, x_1, \dots, x_n, y_1, \dots, y_n$ are pairwise distinct variables *:

(1) $\forall x_1 \ldots \forall x_{n_j} \forall y_1 \ldots \forall y_{n_j}((r_0(x_1, y_1) \wedge \ldots \wedge r_0(x_{n_j}, y_{n_j}) \wedge \wedge\, \alpha s_j(x_1, \ldots, x_{n_j})) \rightarrow \alpha s_j(y_1, \ldots, y_{n_j})), j \leqslant k$;

(2) $\forall x_0 \ldots \forall x_{l_i} \forall y_0 \ldots \forall y_{l_i}((r_0(x_0, y_0) \wedge \ldots \wedge r_0(x_{l_i}, y_{l_i}) \wedge \wedge\, \alpha f_i(x_0, \ldots, x_{l_i})) \rightarrow \alpha f_i(y_0, \ldots, y_{l_i})), i \leqslant m$;

(3) $\forall x_1 \ldots \forall x_{l_i} \exists y \alpha f_i(x_1, \ldots, x_{l_i}, y), i \leqslant m$;

(4) $\forall x_1 \ldots \forall x_{l_i} \forall y \forall z((\alpha f_i(x_1, \ldots, x_{l_i}, y) \wedge \alpha f_i(x_1, \ldots, x_{l_i}, z)) \rightarrow \rightarrow r_0(y, z)), i \leqslant m$;

(5) $\forall x r_0(x, x)$;

(6) $\forall x \forall y(r_0(x, y) \rightarrow r_0(y, x))$;

(7) $\forall x \forall y \forall z((r_0(x, y) \wedge r_0(y, z)) \rightarrow r_0(x, z))$.

It is clear that it follows from condition (2) on Σ^* that for any finite or countable signature Σ there is an interpretation of Σ in Σ^*.

THEOREM 11. *Let Φ be a formula of the calculus of predicates, $\Phi' \equiv \Phi$, Φ' be in reduced nf and α be an interpretation of $\Sigma(\Phi')$ in Σ^*. Then Φ is provable in the calculus of predicates if and only if $\alpha_0 \Phi' \rightarrow \alpha^* \Phi'$ is* CPP-*provable.*

PROOF. By Theorems 1, 6 and 10 it suffices to verify that if Φ' is identically true, then $\alpha_0 \Phi' \rightarrow \alpha^* \Phi'$ is also identically true. For any system $\mathfrak{A}$ of $\Sigma(\Phi') = \langle \{s_0, \ldots, s_k\}, \{f_0, \ldots, f_m\}\ \mu \rangle$ we define a system $\alpha\mathfrak{A}$ of $\alpha\Sigma = \langle \{r_0, \alpha s_0, \ldots, \alpha s_k, \alpha f_0, \ldots, \alpha f_m\}, \varnothing, \alpha\mu \rangle \subseteq \subseteq \Sigma^*$ as follows:

(a) $\alpha A = A$;

(b) $\langle a, b \rangle \in \nu^{\alpha\mathfrak{A}}(r_0) \Leftrightarrow a = b$;

(c) $\nu^{\alpha\mathfrak{A}}(\alpha s_j) = \nu^{\mathfrak{A}}(s_j), j \leqslant k$;

(d) $\nu^{\alpha\mathfrak{A}}(\alpha f_i) = \nu^{\mathfrak{A}}(f_i), i \leqslant m; \mu(f_i) > 0$;

(e) $\nu^{\alpha\mathfrak{A}}(\alpha f_i) = \{\nu^{\mathfrak{A}}(f_i)\}, i \leqslant m, \mu(f_i) = 0$.

It is easy to verify by induction on the length of a formula Ψ of $\Sigma(\Phi')$ in reduced nf that for any interpretation γ in A of free variables of Ψ

$$\mathfrak{A} \models \Psi[\gamma] \Leftrightarrow \alpha\mathfrak{A} \models \alpha^*\Psi[\gamma].$$

---

* The sentence $\alpha_0 \Phi$ depends only on $\Sigma(\Phi)$ and its being true on an algebraic system $\mathfrak{A}$ is equivalent to the fact that $\nu^{\mathfrak{A}}(r_0)$ is an equivalence, that the predicates αS_j and αf_i do not "make different" $\nu^{\mathfrak{A}}(r_0)$-equivalent elements and that relations $\nu^{\mathfrak{A}}(\alpha f_i)$ define l_i-place operations on the classes of $\nu^{\mathfrak{A}}(r_0)$-equivalent elements.

In particular, for any $\gamma\colon FV(\Phi') \to A$ we have

$$\mathfrak{A} \models \neg\Phi'[\gamma] \Rightarrow \alpha\mathfrak{A} \models \neg\alpha^*\Phi'[\gamma]. \qquad (1)$$

It is obvious that $\alpha_0\Phi'$ is true in $\alpha\mathfrak{A}$ and therefore it follows from (1) that if $\alpha_0\Phi' \to \alpha^*\Phi'$ is identically true, then Φ' is identically true.

Suppose that $\alpha_0\Phi' \to \alpha^*\Phi'$ is not identically true. Then for some system $\mathfrak{A}_0$ of $\alpha\Sigma$ and an interpretation γ_0 in A_0 of free variables of Φ' we have $\mathfrak{A}_0 \models \alpha_0\Phi'$ and $\mathfrak{A}_0 \models \neg\alpha^*\Phi'[\gamma_0]$. From the truth in $\mathfrak{A}_0$ of sentences (5) to (7) of the definition of $\alpha_0\Phi'$ it follows that the relation $\nu^{\mathfrak{A}_0}(r_0)$ defines an equivalence on A_0. A $\nu^{\mathfrak{A}_0}(r_0)$-equivalence class containing $a \in A_0$ will be denoted by $\tilde{a}$. We define a system $\mathfrak{B}_0$ of $\Sigma(\Phi')$ as follows:

(a) $B_0 = \{\tilde{a} \mid a \in A_0\}$;

(b) $\langle \tilde{a}_1, \ldots, \tilde{a}_n\rangle \in \nu^{\mathfrak{B}_0}(s_j) \Leftrightarrow \langle a_1, \ldots, a_n\rangle \in \nu^{\mathfrak{A}_0}(\alpha s_j) \quad j \leqslant k$;

(c) $\langle \tilde{a}_1, \ldots, \tilde{a}_{n+1}\rangle \in \nu^{\mathfrak{B}_0}(f_i) \Leftrightarrow \langle a_1, \ldots, a_{n+1}\rangle \in \nu^{\mathfrak{A}_0}(\alpha f_i)$, $i \leqslant m$, $\mu(f_i) = n > 0$;

(d) $\tilde{a} = \nu^{\mathfrak{B}_0}(f_i) \Leftrightarrow a \in \nu^{\mathfrak{B}_0}(\alpha f_i)$, $i \leqslant m$, $\mu(f_i) = 0$.

Since conjunctive terms (1) and (2) of the sentence $\alpha_0\Phi'$ are true on $\mathfrak{A}_0$ it follows that these definitions are correct. Since sentences (3) and (4) are true it follows that $\nu^{\mathfrak{B}_0}(f_i)$, $i \leqslant m$, is an operation on B_0. It is easy to verify by induction on the length of the formula $\Psi(x_1, \ldots, x_n)$ of $\Sigma(\Phi')$ in reduced normal form that for any $a_1, \ldots, a_n \in A_0$

$$\mathfrak{B}_0 \models \Psi(\tilde{a}_1, \ldots, \tilde{a}_n) \Leftrightarrow \mathfrak{A}_0 \models \alpha^*\Psi(a_1, \ldots, a_n).$$

From this it follows that $\mathfrak{B}_0 \models \neg\Phi'[\tilde{\gamma}_0]$, where $\tilde{\gamma}_0(x) = \widetilde{\gamma_0(x)}$, $x \in FV(\Phi')$, i. e. Φ' is not an identically true formula. □

As is to be shown in Sec. 38, there are effectively given sets of formulas for which there is no effective procedure (algorithm) that would establish for any formula of a given set in a finite number of steps whether or not it is an identically true formula. Gödel's completeness theorem enables us to construct from any effectively given signature Σ an effective process (machine) M^{Σ} which enumerates all identically true formulas of Σ, i. e. in the process of work M produces such words $\Phi_0, \ldots, \Phi_n, \ldots$ that $\{\Phi_0, \ldots, \Phi_n, \ldots\}$ is the set of all identically true formulas of Σ.

This process consists in writing out finite sequences of sequents of CP^{Σ} and it produces a word Φ when the sequence it has written out is a linear proof of the sequent $\vdash \Phi$ in CP^{Σ}. Since for any effectively given set of formulas X the passage from a formula $\Phi \in X$ to a formula $\Phi' \equiv \Phi$ in reduced nf and then to a formula $\alpha_0 \Phi' \to \alpha^* \Phi'$ can be made effective, Theorem 11 shows that to be able to enumerate all identically true formulas of any effectively given set of formulas it suffices to construct a machine M enumerating theorems of CPP.

Exercise

1. Let J be a calculus obtained by adding to CPP a symbol of equality and the following axioms:

(a) $\vdash x \approx x$;

(b) $x \approx y, (P)_x^z \vdash (P)_y^z$, where P is an atomic formula of Σ^*. Show that all theorems of CP^{Σ^*} are J-provable.

Chapter 5

MODEL THEORY

24. ELEMENTARY EQUIVALENCE

It was shown in Sec. 16 that the same sentences are true on isomorphic systems. The converse is false for infinite systems. In this section we show (Theorem 1) that the truth on $\mathfrak{A}$ and $\mathfrak{B}$ of the same sentences is equivalent to the existence of a "large enough" supply of finite partial isomorphisms $\mathfrak{A}$ into $\mathfrak{B}$. In particular, if on finite systems $\mathfrak{A}$ and $\mathfrak{B}$ the same sentences are true, then $\mathfrak{A}$ is isomorphic to $\mathfrak{B}$.

DEFINITION. Two algebraic systems $\mathfrak{A}$ and $\mathfrak{B}$ of a signature Σ are said to be *elementarily equivalent* (we write $\mathfrak{A} \equiv \mathfrak{B}$) if for any sentence Φ of Σ

$$\mathfrak{A} \models \Phi \Leftrightarrow \mathfrak{B} \models \Phi.$$

A set of sentences $\{\Phi \mid \mathfrak{A} \models \Phi\}$ of Σ is called an *elementary theory* of the system $\mathfrak{A}$ or simply a *theory* of $\mathfrak{A}$ and is denoted by $\mathrm{Th}(\mathfrak{A})$.

It is clear that the relation $\mathfrak{A} \equiv \mathfrak{B}$ is equivalent to the equation $\mathrm{Th}(\mathfrak{A}) = \mathrm{Th}(\mathfrak{B})$.

DEFINITION. Let $\mathfrak{A}$ and $\mathfrak{B}$ be algebraic systems of $\Sigma = \langle R, F, \mu \rangle$. A distinct-valued mapping $f \colon X \to B$, where $X \subseteq A$, is said to be a *partial isomorphism* of $\mathfrak{A}$ into $\mathfrak{B}$ if for any $a_1, \ldots, a_n \in X$ the following conditions hold:

(1) if $s \in R \cup F$ is not a constant, then

$$\langle a_1, \ldots, a_n \rangle \in \nu^{\mathfrak{A}}(s) \Leftrightarrow \langle fa_1, \ldots, fa_n \rangle \in \nu^{\mathfrak{B}}(s);$$

(2) if $s \in F$ is a constant, then

$$\nu^{\mathfrak{A}}(s) = a_1 \Leftrightarrow \nu^{\mathfrak{B}}(s) = fa_1.$$

(Recall that if $n = 0$, then $\langle a_1, \ldots, a_n \rangle = \langle\,\rangle = \Lambda = \varnothing$.) If X is a finite set, then f is said to be a *finite partial isomorphism*. A set of finite partial isomorphisms of $\mathfrak{A}$ into $\mathfrak{B}$ is denoted by $P(\mathfrak{A}, \mathfrak{B})$.

THEOREM 1. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be systems of Σ. For systems $\mathfrak{A}$ and $\mathfrak{B}$ to be elementarily equivalent it is necessary and sufficient that for* *any* $n \in \omega$ *and any finite signature* $\Sigma_1 \subseteq \Sigma$ *there be nonempty sets* $F_1(\Sigma_1, n), \ldots, F_n(\Sigma_1, n)$ *of finite partial isomorphisms* $\mathfrak{A} \upharpoonright \Sigma_1$ *into* $\mathfrak{B} \upharpoonright \Sigma_1$ *possessing the following property*:

*) *if* $f \in F_i(\Sigma_1, n)$, $1 \leqslant i < n$, *then for any* $a \in A$, and $b \in B$ *there are* $g_1, g_2 \in F_{i+1}(\Sigma_1, n)$ *for which* $a \in \operatorname{dom} g_1$, $b \in \operatorname{rang} g_2$, $f \subseteq g_1$ *and* $f \subseteq g_2$.

PROOF. Sufficiency. We prove by induction on m that if the length of a formula $\Phi(x_1, \ldots, x_k)$ in reduced nf is not greater than m, the sets $F_1(\Sigma(\Phi), n) \subseteq P(\mathfrak{A} \upharpoonright \Sigma(\Phi), \mathfrak{B} \upharpoonright \Sigma(\Phi)), \ldots, F_n(\Sigma(\Phi), n) \subseteq$ $\subseteq P(\mathfrak{A} \upharpoonright \Sigma(\Phi), \mathfrak{B} \upharpoonright \Sigma(\Phi))$ satisfy the condition*) and $i + m \leqslant n$, then for any $f \in F_i(\Sigma(\Phi), n)$ and any $a_1, \ldots, a_k \in \operatorname{dom} f$

$$\mathfrak{A} \vDash \Phi(a_1, \ldots, a_k) \Leftrightarrow \mathfrak{B} \vDash \Phi(fa_1, \ldots, fa_k).$$

If Φ is an atomical formula, then this statement follows from the definition of a partial isomorphism. If $\Phi = \neg\Psi$ or $\Phi = \Psi_1 \tau \Psi_2$, $\tau \in \{\wedge, \vee, \rightarrow\}$, then the statement follows by the induction hypothesis. Since $\forall x \Psi \equiv \neg \exists x \neg \Psi$ for any formula Ψ, it suffices to treat only the case $\Phi(x_1, \ldots, x_k) = \exists y \Psi(y, x_1, \ldots, x_k)$. Let $\mathfrak{A} \vDash \Phi(a_1, \ldots, a_k)$. Then $\mathfrak{A} \vDash \Psi(a_0, a_1, \ldots, a_k)$ for some $a_0 \in A$. Take $g \in F_{i+1}(\Sigma(\Phi), n)$ such that $f \subseteq g$ and $a_0 \in \operatorname{dom} g$. Since the length of Ψ is less than that of Φ, by the induction hypothesis $\mathfrak{B} \vDash \Psi(ga_0, fa_1, \ldots, fa_k)$ and so $\mathfrak{B} \vDash \Phi(fa_1, \ldots, fa_k)$. Let $\mathfrak{B} \vDash \Phi(fa_1, \ldots, fa_k)$. Then $\mathfrak{B} \vDash \Psi(b_0, fa_1, \ldots, fa_k)$ for $b_0 \in B$. Take $g \in F_{i+1}(\Sigma(\Phi), n)$ for which $f \subseteq g$ and $b_0 \in \operatorname{rang} g$. Then by the induction hypothesis $\mathfrak{A} \vDash \Psi(g^{-1}b_0, a_1, \ldots, a_k)$ and hence $\mathfrak{A} \vDash \Phi(a_1, \ldots, a_k)$.

Necessity. Let $\Sigma_1 \subseteq \Sigma$ be a finite signature and let $X(n, m)$ for $n, m \in \omega$ be a maximal set of pairwise nonequivalent formulas Φ of Σ_1 in reduced nf containing $\leqslant n$ quantifiers and $FV(\Phi) \subseteq$ $\subseteq \{v_1, \ldots, v_m\}$. Since there are only a finite number of atomical formulas with variables from the set $\{v_1, \ldots, v_n\}$, it is easy to show by induction on n that for any n and m the set $X(n, m)$ is finite. It is obvious that the function $|X(n, m)|$ is nondecreasing in each of the variables n and m. Let $a_1, \ldots, a_k \in A$ be pairwise distinct. A mapping $f\colon \{a_1, \ldots, a_k\} \to B$ is said to be an (n, m)-*isomorphism* if $k \leqslant m$ and for any formula $\Phi(x_1, \ldots, x_k) \in X(n, m)$

$$\mathfrak{A} \vDash \Phi(a_1, \ldots, a_k) \Leftrightarrow \mathfrak{B} \vDash \Phi(fa_1, \ldots, fa_k).$$

It is clear that any partial isomorphism $f \in P(\mathfrak{A} \upharpoonright \Sigma_1, \mathfrak{B} \upharpoonright \Sigma_1)$ for which $|\mathrm{dom}\, f| \leqslant m$ is a $(0, m)$-isomorphism. For $i = n, n - 1, \ldots, 2, 1$ we shall define nondecreasing functions $g_i : \omega \to \omega$ so that the sets $F_i(\Sigma_1, n) = \{f \mid f$ is a $(g_i(m), m)$-isomorphism for some $m \in \omega\}$ satisfy condition*).

We take as g_n the identity zero. If $1 < i \leqslant n$, $m \in \omega$, we assume

$$g_{i-1}(m) = (g_i(m + 1) \cdot |X(g_i(m + 1), m + 1)|) + 1.$$

If g_i is nondecreasing, then obviously g_{i-1} is also nondecreasing. It follows from $\mathfrak{A} \equiv \mathfrak{B}$ that $f = \varnothing$ is an $(n, 0)$-isomorphism for any $n \in \omega$. Hence the classes $F_1(\Sigma_1, n), \ldots, F_n(\Sigma_1, n)$ are nonempty. Let $f \in F_{i-1}(\Sigma_1, n)$ be a $(g_{i-1}(m), m)$-isomorphism, $1 < i \leqslant n$, $\mathrm{dom}\, f = \{a_1, \ldots, a_k\}$, $k \leqslant m$ and $a \in A$. We denote by $\Phi(v_1, \ldots, v_{k+1})$ the conjunction of all $\Psi(v_1, \ldots, v_{k+1}) \in X(g_i(k + 1), k + 1)$ for which $\mathfrak{A} \models \Psi(a_1, \ldots, a_k, a)$. The number of quantifiers in Φ does not exceed $g_i(k + 1) \cdot |X(g_i(k + 1), k + 1)|$ and therefore there is a formula $\mathrm{X}(v_1, \ldots, v_k) \in X(g_{i-1}(k), k)$ equivalent to a formula $\exists v_{k+1} \Phi(v_1, \ldots, v_{k+1})$. Since $g_{i-1}(k) \leqslant g_{i-1}(m)$, $\mathfrak{A} \models \mathrm{X}(a_1, \ldots, a_k)$ and f is a $(g_{i-1}(m), m)$-isomorphism, we have $\mathfrak{B} \models X(fa_1, \ldots, fa_k)$. Then $\mathfrak{B} \models \Phi(fa_1, \ldots, fa_k, b)$ for some $b \in B$. It follows from the construction of Φ that for any $\Psi \in X(g_i(k + 1), k + 1)$ either $\Phi \to \Psi$ or $\Phi \to \neg \Psi$ is an identically true formula and therefore $g = f \cup \langle a, b \rangle$ is a $(g_i(k + 1), k + 1)$-isomorphism, i. e. is in $F_i(\Sigma_1, n)$. On replacing in the preceding argument $\mathfrak{A}$ by $\mathfrak{B}$ and f by f^{-1} we conclude that for any $b' \in B$ there is $a' \in A$ and that $f \cup \{\langle a', b' \rangle\}$ is in $F_i(\Sigma_1, n)$. □

COROLLARY 1. *If* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are algebraic systems of a finite signature* Σ, *then for* $\mathfrak{A}$ *and* $\mathfrak{B}$ *to be elementarily equivalent it is necessary and sufficient that for any* $n \in \omega$ *there be nonempty sets* $F_1(n) \subseteq P(\mathfrak{A}, \mathfrak{B}), \ldots, F_n(n) \subseteq P(\mathfrak{A}, \mathfrak{B})$ *with the following property*:

*) *if* $f \in F_i(n)$ $1 \leqslant i < n$, $a \in A$ *and* $b \in B$, *then there are* $g_1, g_2 \in F_{i+1}(n)$ *for which* $f \subseteq g_1, f \subseteq g_2$, $a \in \mathrm{dom}\, g_1$ *and* $b \in \mathrm{rang}\, g_2$.

PROOF. As sets $F_1(n), \ldots, F_n(n)$ we take the sets $F_1(\Sigma, n), \ldots, F_n(\Sigma, n)$ of Theorem 1. □

COROLLARY 2. *If* $\mathfrak{A}$, $\mathfrak{B}$ *are algebraic systems of* Σ *and* $\mathfrak{A}$ *is finite, then* $\mathfrak{A} \equiv \mathfrak{B}$ *if and only if* $\mathfrak{A} \simeq \mathfrak{B}$.

PROOF. It is proved in Proposition 16.7 that for any $\mathfrak{A}$ and $\mathfrak{B}$ $\mathfrak{A} \simeq \mathfrak{B}$ implies $\mathfrak{A} \equiv \mathfrak{B}$. Let $\mathfrak{A} \equiv \mathfrak{B}$ and $|A| = m_0 \in \omega$. Since the formula Φ_{m_0} of Proposition 16.9 is true in $\mathfrak{B}$, we have $|B| = m_0$. For every $n \in \omega$ there are only a finite number of pairwise distinct n-place predicates and functions on a finite set, and so there is a countable signature $\Sigma' \subseteq \Sigma$ such that if $s \in R \cup F$, then $\nu^{\mathfrak{A}}(s) = \nu^{\mathfrak{A}}(s')$ for some $s' \in R' \cup F'$. Therefore it suffices to show that $\mathfrak{A} \restriction \Sigma' \simeq \mathfrak{B} \restriction \Sigma'$. Let $\Sigma' = \bigcup\limits_{i \in \omega} \Sigma_i$, where Σ_i is finite and $\Sigma_i \subseteq \Sigma_{i+1}$. We consider the sets of partial isomorphisms $F_j(\Sigma_i, n)$, where $n, i \in \omega$ and $1 \leqslant j \leqslant n$, of Theorem 1. It follows from condition *) of Theorem 1 that for any $n, i \in \omega$, any $k < n$ and any $a_1, \dots, a_k \in A$ there is a mapping $f \in F_{k+1}(\Sigma_i, n)$ for which $a_1, \dots, a_k \in \operatorname{dom} f$. Therefore for any $n > m_0$ there is $f_n \in F_{m_0+1}(\Sigma_n, n)$ which is an isomorphism $\mathfrak{A} \restriction \Sigma_n$ onto $\mathfrak{B}_1 \restriction \Sigma_n$, where $\mathfrak{B}_1 \subseteq \mathfrak{B}$. Since $|B_1| = |A| = |B|$, we have $\mathfrak{B}_1 = \mathfrak{B}$. There are only a finite number of mappings $f\colon A \to B$ and so there is a number $n_0 \in \omega$ such that $f_{n_0}\colon \mathfrak{A} \restriction \Sigma_n \simeq \mathfrak{B} \restriction \Sigma_n$ for every $n \in \omega$. Hence $f_{n_0}\colon \mathfrak{A} \simeq \mathfrak{B}$. $\square$

The notion of elementary equivalence may, from a certain point of view, be even more important than that of isomorphism. The fact is that an isomorphism is defined in terms of the existence of some infinite function while an elementary equivalence is defined in terms of finite functions. Consider algebraic systems $\mathfrak{A}_0$ and $\mathfrak{B}_0$ of an empty signature, in which A_0 consists of all countable ordinals and B_0 consists of all subsets of the natural numbers. It follows from P. Cohen's results on independence in ZFC that $\mathfrak{A}_0 \simeq \mathfrak{B}_0$ can be neither proved nor refuted in ZFC. But by virtue of the "finiteness" of the notion of elementary equivalence for "well formed" systems $\mathfrak{A}$ and $\mathfrak{B}$ the relation $\mathfrak{A} \equiv \mathfrak{B}$ can be proved or refuted in ZFC. In particular, it is easy to show that $\mathfrak{A}_0 \equiv \mathfrak{B}_0$. One should not forget, of course, that the concept of isomorphism plays a role of exceptional importance in algebra, for example, since it is the "limit" for various classifications of algebraic systems.

While elementary equivalence is a weakening of the notion of isomorphism, the following concept is a strengthening of the notion of subsystem.

DEFINITION. A subsystem $\mathfrak{B} \subseteq \mathfrak{A}$ of a system of Σ is said to be an *elementary subsystem* (we write $\mathfrak{B} \prec \mathfrak{A}$) if for any formula $\Phi(x_1, \ldots, x_n)$ of Σ and any $b_1, \ldots, b_n \in B$

$$\mathfrak{B} \models \Phi(b_1, \ldots, b_n) \Leftrightarrow \mathfrak{A} \models \Phi(b_1, \ldots, b_n). \tag{1}$$

PROPOSITION 1. *Let $\mathfrak{A}$ be an algebraic system of Σ and $\mathfrak{B} \subseteq \mathfrak{A}$. For $\mathfrak{B} \prec \mathfrak{A}$ to hold it is necessary and sufficient that for any formula $\Phi(x_0, \ldots, x_n)$ of Σ and any $b_1, \ldots, b_n \in B$ $\mathfrak{A} \models \exists x_0 \Phi(x_0, b_1, \ldots, b_n) \Rightarrow (\mathfrak{A} \models \Phi(b_0, b_1, \ldots, b_n)$ for some $b_0 \in B)$.*

PROOF. We show by induction on the length of a formula $\Phi(x_1, \ldots, x_n)$ of Σ that for any $b_1, \ldots, b_n \in B$ (1) is true. If Φ is atomic, then (1) follows from the definition of a subsystem. If $\Phi = \neg \Psi$ or $\Phi = \Psi_1 \tau \Psi_2$ for $\tau \in \{\wedge, \vee, \rightarrow\}$, then (1) follows from the induction hypothesis. Since $\forall x \Psi \equiv \neg \exists x \neg \Psi$, it suffices to treat only the case $\Phi(x_1, \ldots, x_n) = \exists x_0 \Psi(x_0, \ldots, x_n)$, but in this case (1) follows from the hypothesis of the proposition and the induction hypothesis. □

PROPOSITION 2. *Let $\mathfrak{A}$ be an algebraic system of Σ and $\mathfrak{B} \subseteq \mathfrak{A}$. If for any finite signature $\Sigma_1 \subseteq \Sigma$, any $b_1, \ldots, b_n \in B$ and any $a \in A$ there is an automorphism f of a system $\mathfrak{A} \restriction \Sigma_1$ such that $fb_1 = b_1, \ldots, fb_n = b_n$ and $fa \in B$, then $\mathfrak{B} \prec \mathfrak{A}$.*

PROOF. We use Proposition 1. Let $\mathfrak{A} \models \exists x_0 \Phi(x_0, b_1, \ldots, b_n)$. Then $\mathfrak{A} \models \Phi(a, b_1, \ldots, b_n)$ for some $a \in A$. Let f be an automorphism of a system $\mathfrak{A} \restriction \Sigma(\Phi)$ leaving $b_1, \ldots, b_n$ fixed and $fa \in B$. From Proposition 16.7 we get $\mathfrak{A} \models \Phi(fa, b_1, \ldots, b_n)$. □

It is clear that $\mathfrak{B} \prec \mathfrak{A}$ implies $\mathfrak{B} \equiv \mathfrak{A}$. In general the converse is false. Consider, for example, systems $\langle Q^{(1)}; \leqslant \rangle$ and $\langle Q^{(2)}; \leqslant \rangle$, where $Q^{(1)}$, $Q^{(2)}$ are sets of rational numbers not less than 1 and not less than 2 respectively and $\leqslant$ is the usual "less than or equal to" relation on numbers. By Proposition 15.4 the systems $\langle Q^{(1)}; \leqslant \rangle$ and $\langle Q^{(2)}; \leqslant \rangle$ are isomorphic and hence elementarily equivalent. However, in the subsystem $\langle Q^{(2)}; \leqslant \rangle$ of the system $\langle Q^{(1)}; \leqslant \rangle$ the formula $\Phi(v_1) = \forall v_0 (v_0 \leqslant v_1 \rightarrow v_0 \approx v_1)$ is true on the element 2 and in the system $\langle Q^{(1)}; \leqslant \rangle$ this formula is false on the same element 2. Thus $\langle Q^{(2)}; \leqslant \rangle \prec \langle Q^{(1)}; \leqslant \rangle$ fails.

EXAMPLE 1. Let $\mathfrak{A}$ be a countable dense linear ordering and $\mathfrak{B}$ be a dense-in-$\mathfrak{A}$ ordering (i. e. let $\mathfrak{B} \subseteq \mathfrak{A}$ and for any $a < b$ in A there be $c \in B$ such that $a < c < b$). Then ($\mathfrak{B}$ contains the end elements of $\mathfrak{A}$) $\Leftrightarrow$ $\mathfrak{B} \prec \mathfrak{A}$.

To prove $\Leftarrow$ we notice that since $\mathfrak{A} \equiv \mathfrak{B}$, $\mathfrak{A}$ and $\mathfrak{B}$ have the same ends. Now suppose, for example, that b_0 is the first element of $\mathfrak{B}$. Then $\mathfrak{B} \models \forall v_0(v_0 \leqslant b_0 \to v_0 \approx b_0)$. By virtue of $\mathfrak{B} \prec \mathfrak{A}$ we have $\mathfrak{A} \models \forall v_0(v_0 \leqslant b_0 \to v_0 \approx b_0)$ and hence b_0 is the first element of $\mathfrak{A}$. To prove $\Rightarrow$ it is necessary to use Proposition 2. The desired isomorphism f is constructed the same way as in Proposition 15.4.

EXAMPLE 2. Let $\mathfrak{A}$ be a free group with free generators $\{a_i \mid i \in \in I\}$ and let $I' \subseteq I$ be an infinite set. Then a group $\mathfrak{B} \subseteq \mathfrak{A}$ generated in $\mathfrak{A}$ by a set $\{a_i \mid i \in I'\}$ is an elementary subgroup of $\mathfrak{A}$. To prove this we use Proposition 2. Let $b_1, \ldots, b_n \in B$ and $a \in A$. Then there are finite sets $X \subseteq \{a_i \mid i \in I'\}$ and $Y \subseteq \{a_i \mid i \in \in I\} \setminus X$ such that $b_1, \ldots, b_n \in A(X)$ and $a \in A(X \cup Y)$. Consider a distinct-valued mapping f of the set $\{a_i \mid i \in I\}$ onto itself leaving the elements of X fixed and mapping Y into $\{a_i \mid i \in I'\}$. Then f is uniquely extended up to an automorphism of the group $\mathfrak{A}$ which satisfies the hypothesis of Proposition 2.

Although in many cases the test of Proposition 2 is easy to apply, it is not necessary (see Exercise 2). Note that the possibility of replacing in Example 2 the condition that I' is infinite by $|I'| > > 1$ is a standing problem.

There is no analogue of Proposition 15.2 for the relation $\prec$ (see Exercise 2) while for Proposition 15.3 the corresponding statement holds. A set $\{\mathfrak{A}_i \mid i \in I\}$ of algebraic systems is said to be *elementarily directed* if for any $i, j \in I$ there is $k \in I$ such that $\mathfrak{A}_i \prec \prec \mathfrak{A}_k$ and $\mathfrak{A}_j \prec \mathfrak{A}_k$.

PROPOSITION 3. *If* $\{\mathfrak{A}_i \mid i \in I\}$ *is an elementarily directed set of algebraic systems of* Σ, *then* $\mathfrak{A}_j \prec \mathfrak{A} = \bigcup\limits_{i \in I} \mathfrak{A}_i$, $j \in I$.

PROOF. For $\mathfrak{B} = \mathfrak{A}_j$ equivalence (1) will be proved by induction on the length of Φ. It suffices, as in the proof of Proposition 1, to treat the case $\Phi = \exists x \Psi$. Let $\mathfrak{A} \models \exists x \Psi(x, a_1, \ldots, a_n)$, where $a_1, \ldots \ldots, a_n \in A_j$. Then $\mathfrak{A} \models \Psi(a, a_1, \ldots, a_n)$ for some $a \in A_i$. Take $k \in I$ for which $\mathfrak{A}_i \prec \mathfrak{A}_k$ and $\mathfrak{A}_j \prec \mathfrak{A}_k$. By the induction hypothesis $\mathfrak{A}_k \models \models \Psi(a, a_1, \ldots, a_n)$ and hence $\mathfrak{A}_k \models \exists x \Psi(x, a_1, \ldots, a_n)$. Since $\mathfrak{A}_j \prec \prec \mathfrak{A}_k$, we have $\mathfrak{A}_j \models \exists x \Psi(x, a_1, \ldots, a_n)$. Conversely, let $\mathfrak{A}_j \models \models \exists x \Psi(x, a_1, \ldots, a_n)$. Then $\mathfrak{A}_j \models \Psi(a, a_1, \ldots, a_n)$ for some $a \in A_j$

and by the induction hypothesis $\mathfrak{A} \models \Psi(a, a_1, \ldots, a_n)$ and therefore $\mathfrak{A} \models \exists x\Psi(x, a_1, \ldots, a_n)$. $\square$

Although there is no analogue of Proposition 15.2 for $\prec$, a weaker variant of the corresponding statement is very important.

THEOREM 2. *Let $\mathfrak{A}$ be an algebraic system of Σ and $X \subseteq A$. Then there is an elementary subsystem $\mathfrak{B} \prec \mathfrak{A}$ such that $X \subseteq B$ and* $|B| = \max(|X|, |\Sigma|, \omega)$.

PROOF. Set $X_0 = X$. Suppose X_n is already defined. For any formula $\Psi = \exists y\Phi(y, x_1, \ldots, x_k)$ of Σ and any interpretation $\gamma: \{x_1, \ldots, x_k\} \to A$ we choose an element $a(\Psi, \gamma) \in A$ such that if $\mathfrak{A} \models \exists x\Phi(x, \gamma x_1, \ldots, \gamma x_k)$, then $\mathfrak{A} \models \Phi(a(\Psi, \gamma), \gamma x_1, \ldots, \gamma x_k)$. Set $X_{n+1} = X_n \cup \{a(\Psi, \gamma) \mid \Psi = \exists x\Phi \in F(\Sigma), \gamma: FV(\Psi) \to X_n\}$. It is clear that the subsystem $\mathfrak{B} \subseteq \mathfrak{A}$ with carrier $\bigcup\limits_{n \in \omega} X_n$ satisfies the hypothesis of Proposition 1 and, hence, $\mathfrak{B} \prec \mathfrak{A}$. If $\lambda = \max(|X|, |\Sigma|, \omega)$ then $|F(\Sigma)| \leqslant \lambda$ and $|X_0| \leqslant \lambda$. If $|X_n| \leqslant \lambda$, then the power of a set Y_n of interpretations γ of variables in X_n with a finite domain is at most $\left|\bigcup\limits_{m \in \omega} X_n^m\right|$. Since $|X_n^m| \leqslant \max(|X_n|, \omega)$, we have $|Y_n| \leqslant \lambda \cdot \omega = \lambda$, and so $|X_{n+1}| \leqslant |F(\Sigma)| \cdot |Y_n| \leqslant \lambda^2 = \lambda$. Therefore $|B| \leqslant \lambda \cdot \omega = \lambda$. $\square$

DEFINITION. Let $\mathfrak{A}$ be an algebraic system of Σ and $X \subseteq A$. We take a set $C_X = \{c_a \mid a \in X\}$ not intersecting with $R \cup F$ and $c_a \neq c_b$ for $a \neq b$. We define a signature Σ_X to be obtained from Σ by adding elements of C_X as new constants. We denote by $\mathfrak{A}_X$ an expansion of the system $\mathfrak{A}$ to Σ_X in which a constant c_a, $a \in X$, is interpreted by an element a. A set $D(\mathfrak{A}, X)$ of atomical sentences of Σ_X true in the system $\mathfrak{A}_X$ is said to be a *diagram of a set X* in $\mathfrak{A}$. If in the definition of $D(\mathfrak{A}, X)$ we replace "atomical sentences" by "sentences", we obtain a definition of a *complete diagram $D^*(\mathfrak{A}, X)$ of the set X in* $\mathfrak{A}$. A diagram (a complete diagram) of A in $\mathfrak{A}$ is said to be a *diagram* (*a complete diagram*) of $\mathfrak{A}$ and denoted by $D(\mathfrak{A})$ (by $D^*(\mathfrak{A})$ respectively).

PROPOSITION 4. (a) *If $\mathfrak{A}$ is an algebraic system of Σ and $\mathfrak{B}$ is a model of a diagram $D(\mathfrak{A})$ of (a complete diagram $D^*(\mathfrak{A})$) of Σ_A, then $\mathfrak{A} \simeq \mathfrak{B}_1 \upharpoonright \Sigma$ for some $\mathfrak{B}_1 \subseteq \mathfrak{B}$ (some $\mathfrak{B}_1 \prec \mathfrak{B}$).*

(b) *If $\mathfrak{A} \subseteq \mathfrak{B}$ are algebraic systems of Σ, then*

$$\mathfrak{A} \prec \mathfrak{B} \Leftrightarrow \mathfrak{A}_A \equiv \mathfrak{B}_A.$$

PROOF. (a) It is obvious that a mapping assigning to an element $a \in A$ an element $\nu^{\mathfrak{B}}(c_a)$ will be the desired isomorphism. (b) Is immediated from the definitions. □

Theorem 2 allows us to "descend" the powers, preserving the elementary properties. The following theorem allows us to "ascend".

THEOREM 3. *If* $\mathfrak{A}$ *is an infinite system of* Σ *and* λ *is a cardinal not less than* $\max\{|A|, |\Sigma|\}$, *then there is a system* $\mathfrak{B}$ *such that* $\mathfrak{A} \prec \mathfrak{B}$ *and* $|B| = \lambda$.

PROOF. Take a set C of symbols of constants of power λ not intersecting with the set $R \cup F$. Consider a set

$$Y = D^*(\mathfrak{A} \cup \{\neg c_1 \approx c_2 | c_1, c_2 \in C, c_1 \neq c_2\}.$$

Since $\mathfrak{A}$ is infinite, for any finite subset $X \subseteq Y$ the system $\mathfrak{A}$ can be expanded to a model of X. By the compactness theorem there is a model $\mathfrak{B}_1$ of the set Y of $\Sigma_{A \cup C}$. It is obvious that $|B_1| \geqslant \lambda$. By Theorem 2 there is $\mathfrak{B}_2 \prec \mathfrak{B}_1, |B_2| = \lambda$. By Proposition 4 (a) there is $\mathfrak{B}_3 \prec \mathfrak{B}_2$, and an isomorphism $f_1 : \mathfrak{A} \simeq \mathfrak{B}_3 \upharpoonright \Sigma$. Now we need only to replace in the system $\mathfrak{B}_2 \upharpoonright \Sigma$ the elements $b \in B_3$ by $f_1^{-1} b$ to obtain the desired $\mathfrak{B}$. To avoid collision in such a rewriting we proceed as follows. We take a set Z for which $Z \cap A = \varnothing$ and $|Z| = |B_2 \setminus B_3|$. Let f be a distinct-valued mapping of a set $B = A \cup Z$ onto the set B_2 and $f_1 \subseteq f$. We define a system $\mathfrak{B} = \langle B, \nu^{\mathfrak{B}} \rangle$ of Σ as follows:

(a) if $s \in R \cup F$ is not a constant, then

$$\langle b_1, \ldots, b_n \rangle \in \nu^{\mathfrak{B}}(s) \Leftrightarrow \langle fb_1, \ldots, fb_n \rangle \in \nu^{\mathfrak{B}_2}(s);$$

(b) if $s \in F$ is a constant, then

$$\nu^{\mathfrak{B}}(s) = f^{-1}(\nu^{\mathfrak{B}_2}(s)).$$

It is clear that f is an isomorphism of $\mathfrak{B}$ onto $\mathfrak{B}_2 \upharpoonright \Sigma$ and $\mathfrak{A} \subseteq \mathfrak{B}$. Let $\Phi(x_0, x_1, \ldots, x_n) \in F(\Sigma)$; $b_1, \ldots, b_n \in A$ and

$$\mathfrak{B} \models \exists x_0 \Phi(x_0, b_1, \ldots, b_n).$$

Then $\mathfrak{B}_2 \models \exists x_0 \Phi(x_0, fb_1, \ldots, fb_n)$. Since $fb_1, \ldots, fb_n \in B_3$ and $\mathfrak{B}_3 \prec \mathfrak{B}_2$, there is $b_0 \in B_3$ such that $\mathfrak{B}_2 \models \Phi(b_0, fb_1, \ldots, fb_n)$. The mapping f^{-1} is an isomorphism of $\mathfrak{B}_2 \upharpoonright \Sigma$ onto $\mathfrak{B}$ and therefore $\mathfrak{B} \models \Phi(f^{-1}b_0, b_1, \ldots, b_n)$. Since $f^{-1}b_0 \in A$, by Proposition 1 we have $\mathfrak{A} \prec \mathfrak{B}$. From $|B_2| = \lambda$ and $\mathfrak{B}_2 \simeq \mathfrak{B}$ we get $|B| = \lambda$. □

Exercises

1. Show that for systems $\mathfrak{A} \subseteq \mathfrak{B}$ of Σ we have $\mathfrak{A} < \mathfrak{B}$ if one of the following conditions holds:

(a) Σ contains only an infinite set of constants. The values of constants in $\mathfrak{B}$ form an infinite set.

(b) Σ contains only the symbols of one-place predicates r_k, $k \in \omega$. Consider the set $2^\omega = \{\nu \mid \nu\colon \omega \to \{0, 1\}\}$. Let $\mathfrak{B}$ be an arbitrary system of Σ. For any $\nu \in 2^\omega$ we define a set $\mathfrak{B}(\nu) = \{b \mid \text{for all } n \in \omega\ \mathfrak{B} \models r_n(b) \text{ if } \nu(n) = 1 \text{ and } \mathfrak{B} \models \neg r_n(b) \text{ if } \nu(n) = 0\}$. It is clear that for distinct $\nu_1, \nu_2 \in 2^\omega$ the sets $\mathfrak{B}(\nu_1)$ and $\mathfrak{B}(\nu_2)$ do not intersect. Suppose that for all $\nu \in 2^\omega \mathfrak{B}(\nu) \subseteq A$ if $\mathfrak{B}(\nu)$ is a finite set and $A \cap \mathfrak{B}(\nu)$ is an infinite set if $\mathfrak{B}(\nu)$ is infinite.

(c) Σ contains only one symbol $\sim$ of a two-place relation which is interpreted in $\mathfrak{B}$ as an equivalence with an infinite number of infinite equivalence classes. The class A contains an infinite number of equivalence classes of the system $\mathfrak{B}$. (*Hint.* Use Proposition 4(b) and Theorem 1.)

2. Using the example of Exercise 1(c) show that

(a) the property of being elementary is not necessary for the subsystems of Proposition 2 (*Hint.* Suppose $|A| = \omega$ and all equivalence classes contained in $B \setminus A$ are noncountable.);

(b) for some system $\mathfrak{B}$ and an infinite set $X \subseteq B$ there is no elementary subsystem $\mathfrak{A} < \mathfrak{B}$ containing X that is minimal with respect to the inclusion $\subseteq$.

25. AXIOMATIZABLE CLASSES

DEFINITION. A class K of algebraic systems is said to be *axiomatizable* if there is a signature Σ and a set of sentences Z of Σ such that for any system

$$\mathfrak{A} \in K \Leftrightarrow (\text{the signature of } \mathfrak{A} \text{ is } \Sigma \text{ and } \mathfrak{A} \models \Phi \text{ for all } \Phi \in Z). \qquad (1)$$

If (1) holds for a class K, then Σ is said to be the *signature of* K and the set Z is said to be the *set of axioms for* K (we write $K = K_\Sigma(Z)$). If all systems of the class K have a signature Σ, then the set of sentences of the signature Σ true on all the systems of K is said to be an *elementary theory of* K or simply a *theory of* K and denoted by $\mathrm{Th}(K)$.

Note the obvious property of theories: if $K_1 \subseteq K_2$ are classes of algebraic systems of Σ, then $\mathrm{Th}(K_2) \subseteq \mathrm{Th}(K_1)$.

PROPOSITION 1. *Let K be a class of algebraic systems of a signature Σ.*

(a) *The class K is axiomatizable if and only if $K = K_\Sigma(\mathrm{Th}(K))$.*

(b) *There is an $\subseteq$-minimal axiomatizable class K_1 of Σ containing K.*

PROOF. (a) Let $K = K_\Sigma(Z)$. Since $Z \subseteq \mathrm{Th}(K)$, we have $K_\Sigma(\mathrm{Th}(K)) \subseteq K$. The converse inclusion $K \subseteq K_\Sigma(\mathrm{Th}(K))$ is obvious.

(b) It is necessary to take $K_\Sigma(\mathrm{Th}(K))$ as K_1. Indeed, if K_2 is an axiomatizable class of Σ and $K \subseteq K_2$, then $\mathrm{Th}(K_2) \subseteq \mathrm{Th}(K)$. Hence $K_\Sigma(\mathrm{Th}(K)) \subseteq K_\Sigma(\mathrm{Th}(K_2)) = K_2$. □

We shall say that a class of algebraic systems is closed under elementary equivalence (under isomorphisms, subsystems, ultraproducts and so on) if together with algebraic systems $\mathfrak{A}_i$ $i \in I$ it contains all systems elementarily equivalent to them (all isomorphic systems, all their subsystems, the ultraproduct D-prod $\mathfrak{A}_i$ and so on).

We give one useful characterization of axiomatizable classes.

THEOREM 4. *A class K of algebraic systems of a signature Σ is axiomatizable if and only if it is closed under an elementary equivalence and ultraproducts.*

PROOF. Let K be an axiomatizable class. It is obvious that K is closed under an elementary equivalence. The closure of K under ultraproducts follows from Theorem 17.1. Let K be closed under an elementary equivalence and ultraproducts. It suffices to show that $K_\Sigma(\mathrm{Th}(K)) \subseteq K$. Let $\mathfrak{A} \in K_\Sigma(\mathrm{Th}(K))$. For each $\Phi \in \mathrm{Th}(\mathfrak{A})$ consider the sets $u_\Phi = \{\Psi \in \mathrm{Th}(\mathfrak{A}) \mid \rhd\ \Psi \to \Phi\}$. It is clear that $X = \{u_\Phi \mid \Phi \in \mathrm{Th}(\mathfrak{A})\}$ is a family of sets with the finite intersection property. By Proposition 12.1 there is an ultrafilter D on the set $\mathrm{Th}(\mathfrak{A})$ such that $X \subseteq D$. For any $\Phi \in \mathrm{Th}(\mathfrak{A})$ there is a system $\mathfrak{B}_\Phi \in K$ on which Φ is true since otherwise $\neg\Phi \in \mathrm{Th}(K)$, which contradicts $\mathfrak{A} \in K_\Sigma(\mathrm{Th}(K))$. We show that $\mathfrak{A} \equiv D$-prod $\mathfrak{B}_\Phi$ and this will prove the theorem. If $\mathfrak{A} \models \Phi_0$, then $\mathfrak{B}_\Psi \models \Phi_0$ for all $\Psi \in u_{\Phi_0}$. Since $u_{\Phi_0} \in D$, by Theorem 17.1 we get D-prod $\mathfrak{B}_\Phi \models \Phi_0$. If $\mathfrak{A} \models \Phi_0$ does not hold, then $\mathfrak{A} \models \neg\Phi_0$ and by what has just been proved D-prod $\mathfrak{B}_\Phi \models \neg\Phi_0$. Hence D-prod $\mathfrak{B}_\Phi \models \Phi_0$ fails. □

PROPOSITION 2. *The intersection of any set of axiomatizable classes of Σ and the union of a finite number of axiomatizable classes of Σ are axiomatizable classes.*

PROOF. If $K_i = K_\Sigma(Z_i)$, $i \in I$, then obviously $\bigcap_{i \in I} K_i = K_\Sigma\left(\bigcup_{i \in I} Z_i\right)$. Let $K_1 = K_\Sigma(Z_1)$ and $K_2 = K_\Sigma(Z_2)$. Consider a set $Z = \{\Phi \vee \Psi \mid \Phi \in Z_1, \Psi \in Z_2\}$. We show that $K_1 \cup K_2 = K_\Sigma(Z)$. The inclusion $K_1 \cup K_2 \subseteq K_\Sigma(Z)$ is obvious. Let $\mathfrak{A} \neq K_1 \cup K_2$ and let the signature of $\mathfrak{A}$ be Σ. Then there are $\Phi_0 \in Z_1$ and $\Psi_0 \in Z_2$ such that $\mathfrak{A} \models \Phi_0 \wedge \neg \Psi_0$. Since $\Phi \vee \Psi \in Z$, we have $\mathfrak{A} \notin K_\Sigma(Z)$. □

DEFINITION. If K is a class of algebraic systems and $K = K_\Sigma(Z)$ for some finite set of axioms Z, then K is said to be a *finitely axiomatizable* class.

Notice that if K is finitely axiomatizable, then by taking the conjunction of a finite set Z of axioms for K we obtain a set of axioms $\{\Phi\}$ for K consisting of one sentence Φ.

If K is a class of algebraic systems of a signature Σ, then by $\overline{K}$ we denote the complement of K in the class $K_\Sigma(\varnothing)$ of all systems of Σ.

PROPOSITION 3. *Let K be a class of algebraic systems of a signature Σ. The class K is finitely axiomatizable if and only if K and $\overline{K}$ are axiomatizable.*

PROOF. If K is finitely axiomatizable, then $K = K_\Sigma(\{\Phi\})$ for some sentence Φ of Σ. Hence $\overline{K} = K_\Sigma(\{\neg\Phi\})$. Let K and $\overline{K}$ be axiomatizable. Since $K \cap \overline{K} = \varnothing$, $K = K_\Sigma(\mathrm{Th}(K)$ and $\overline{K} = K_\Sigma(\mathrm{Th}(\overline{K}))$, by the compactness theorem there are finite sets $X \subseteq \mathrm{Th}(K)$ and $Y \subseteq \mathrm{Th}(\overline{K})$ such that $X \cup Y$ has no model. Since $\mathrm{Th}(K)$ and $\mathrm{Th}(\overline{K})$ are closed under conjunctions, it may be assumed that $X = \{\Phi\}$ and $Y = \{\Psi\}$. Since $\Phi \wedge \Psi$ is an identically false formula and $\Phi \in \mathrm{Th}_\Sigma(K)$, a sentence $\Phi \wedge \neg\Psi$ is true on all systems of K. Conversely, if the sentence $\Phi \wedge \neg\Psi$ is true on the system $\mathfrak{A}$ of Σ, then $\mathfrak{A} \notin \overline{K}$ and hence $\mathfrak{A} \in K$. So $K = K_\Sigma(\{\Phi \wedge \neg\Psi\})$. □

DEFINITION. A formula Φ is said to be an *$\forall$-formula* (an *$\exists$-formula*, and *$\forall\exists$-formula*) if $\Phi = \forall x_1 \ldots \forall x_k \Psi$ ($\Phi = \exists x_1 \ldots \ldots \exists x_k \Psi$, $\Phi = \forall x_1 \ldots \forall x_k \exists y_1 \ldots \exists y_n \Psi$), where Ψ is a quantifier-free formula. A class K of algebraic systems is said to be *$\forall$-axiomatizable* (*$\exists$-axiomatizable*, *$\forall\exists$-axiomatizable*) if $K = K_\Sigma(Z)$, where Z are sets of $\forall$-sentences ($\exists$-sentences, $\forall\exists$-sentences) of a signature Σ.

PROPOSITION 4. (a) *Let* $\Phi(x_1, \ldots, x_k)$ *be an* $\forall$*-formula* ($\exists$*-formula*) *of a signature* Σ *and let* $\mathfrak{A} \subseteq \mathfrak{B}$ *be algebraic systems of* Σ, $a_1, \ldots, a_k \in A$. *Then if* $\Phi(a_1, \ldots, a_k)$ *is true in* $\mathfrak{B}$ (*in* $\mathfrak{A}$), $\Phi(a_1, \ldots$ $\ldots, a_k)$ *is true in* $\mathfrak{A}$ (*in* $\mathfrak{B}$).

(b) *Let* $\{\mathfrak{A}_i \mid i \in I\}$ *be a directed family of algebraic systems of a signature* Σ *and let an* $\forall\exists$*-sentence* Φ *of* Σ *be true in all* $\mathfrak{A}_i$, $i \in I$. *Then* Φ *is true in* $\mathfrak{A} = \bigcup_{i \in I} \mathfrak{A}_i$.

PROOF. (a) Since the value $t^{\mathfrak{A}}[\gamma]$ of a term t for an interpretation γ in A coincides with the value $t^{\mathfrak{B}}[\gamma]$, (a) holds for atomic formulas Φ. For quantifier-free formulas (a) is obtained by induction on the length of Φ. Now it only remains to use the definition of the truth of formulas with quantifiers $\forall$ and $\exists$.

(b) Let $\Phi = \forall x_1 \ldots \forall x_k \exists y_1 \ldots \exists y_n \Psi(x_1, \ldots, x_k, y_1, \ldots, y_n)$, where Ψ is a quantifier-free formula, be true on all $\mathfrak{A}_i$, $i \in I$. Take arbitrary $a_1, \ldots, a_k \in A$. Then $a_1, \ldots, a_k \in A_i$ for some $i \in I$ and hence $\mathfrak{A}_i \vDash \exists y_1 \ldots \exists y_m \Psi(a_1, \ldots, a_k, y_1, \ldots, y_m)$. Since $\mathfrak{A}_i \subseteq \mathfrak{A}$, by virtue of (a) we have $\mathfrak{A} \vDash \exists y_1 \ldots \exists y_m \Psi(a_1, \ldots, a_k, y_1, \ldots, y_m)$. □

LEMMA 1. *Let* Γ *be a set of sentences of a signature* Σ *and let* $\Psi_0(x_1, \ldots, x_k)$ *be formulas of* Σ. *If for any models* $\mathfrak{A} \subseteq \mathfrak{B}$ *of* Γ *having the signature* Σ *and any* $a_1, \ldots, a_k \in A$ *the truth of* $\Psi_0(a_1, \ldots, a_k)$ *in* $\mathfrak{B}$ (*in* $\mathfrak{A}$) *implies the truth of* $\Psi_0(a_1, \ldots, a_k)$ *in* $\mathfrak{A}$ (*in* $\mathfrak{B}$), *then there is an* $\forall$*-formula* ($\exists$*-formula*) $X_0(x_1, \ldots, x_k)$ *of* Σ *for which* $\Gamma \rhd (\Psi_0 \to X_0) \wedge (X_0 \to \Psi_0)$.

PROOF. Consider a set $Z = \{\Phi(x_1, \ldots, x_k) \mid \Phi$ is an $\forall$-formula of Σ and $\Gamma \rhd \Psi_0 \to \Phi\}$. If $Z \cup \Gamma$ is incompatible, then $\Gamma \cup \{\Psi_0\}$ is incompatible and $\forall v_0(\neg v_0 \approx v_0)$ may be taken as X_0. Let $\mathfrak{A}$ be a model of $Z \cup \Gamma$ of the signature Σ and let $b_1, \ldots, b_k$ be elements of A such that $\mathfrak{A} \vDash \Phi(b_1, \ldots, b_k)$ for any formula $\Phi(x_1, \ldots, x_k) \in Z$. Suppose that the set $D(\mathfrak{A}) \cup \Gamma \cup \{\Psi_0(c_{b_1}, \ldots, c_{b_k})\}$ is incompatible. Then there is a proof D_0 of a sequent $\Phi_0 \vdash \Psi_0(c_{b_1}, \ldots, c_{b_k}) \to$ $\to \neg \Phi_1$ in CP^{Σ_A}, where Φ_0 is a conjunction of some elements of Γ and Φ_1 is a conjunction of some elements of $D(\mathfrak{A})$. On replacing in D_0 all the constants $c_{b_1}, \ldots, c_{b_k}, c_{b_{k+1}}, \ldots, c_{b_n}$ of C_A by variables $y_1, \ldots, y_n$ not occurring in the elements of the tree D_0 and different from $x_1, \ldots, x_k$ we obtain a proof D_1 of the sequent $\Phi_0 \vdash$ $\vdash \Psi_0(y_1, \ldots, y_k) \to \neg \Phi_2$ in CP^{Σ}, where Φ_2 is obtained from Φ_1 by replacing the constants $c_{b_1}, \ldots, c_{b_n}$ by the variables $y_1, \ldots$

$\ldots, y_n$ respectively.* The sequent $\Phi_0 \vdash \Psi_0(y_1, \ldots, y_k) \to \forall y_{k+1} \ldots$ $\ldots \forall y_n \neg \Phi_2$ is then CP$^\Sigma$-provable. From Proposition 18.4 (g) and Theorem 22.9 we obtain $\forall y_{k+1} \ldots \forall y_n (\neg \Phi_2)^{y_1, \ldots, y_k}_{x_1, \ldots, x_k} \in Z$. Then $\mathfrak{A} \models \forall y_{k+1} \ldots \forall y_n \neg \Phi_2[\gamma]$, where $\gamma(y_i) = b_i$, $1 \leqslant i \leqslant n$. Since Φ_1 is a conjunction of elements of $D(\mathfrak{A})$ and $\Phi_1 = (\Phi_2)^{y_1, \ldots, y_n}_{c_{b_1}, \ldots, c_{b_n}}$, we have $\mathfrak{A} \models \Phi_2[\gamma]$, a contradiction. Thus the set $X = D(\mathfrak{A}) \cup \Gamma \cup \{\Psi_0(c_{b_1}, \ldots, c_{b_n})\}$ is compatible. By the theorem on the existence of a model there is a model $\mathfrak{B}$ of X. It is clear that a mapping f assigning to an element $a \in A$ an element $\nu^{\mathfrak{B}}(c_a)$ is an isomorphism of $\mathfrak{A}$ onto a subsystem $\mathfrak{B}_1 \subseteq \mathfrak{B} \upharpoonright \Sigma$ with carrier $B_1 = \{\nu^{\mathfrak{B}}(c_a) \mid a \in A\}$. The hypothesis of the lemma yields $\mathfrak{B}_1 \models \Psi_0(\nu^{\mathfrak{B}}(c_{b_1}), \ldots, \nu^{\mathfrak{B}}(c_{b_k}))$ and, hence, $\mathfrak{A} \models \Psi_0(b_1, \ldots, b_k)$. Since $\mathfrak{A}$ is an arbitrary model of $Z \cup \Gamma$ and $b_1, \ldots, b_k$ are arbitrary elements of A for which $\mathfrak{A} \models \Phi(b_1, \ldots, b_k)$, $\Phi \in Z$, by Corollary 22.4 $Z \cup \Gamma \rhd \Psi_0(x_1, \ldots, x_k)$. Hence, there is a finite set $Z_0 \subseteq Z$ such that $Z_0 \cup \Gamma \rhd \Psi_0(x_1, \ldots, x_k)$. If $X_0(x_1, \ldots, x_k)$ is an $\forall$-formula equivalent to a conjunction of elements of Z_0, then it is obvious that $\Gamma \rhd (X_0 \to \Psi_0) \wedge (\Psi_0 \to X_0)$.

The proof of the corresponding statement for $\exists$-formulas is obtained from the foregoing by considering $\neg \Psi_0$ instead of Ψ_0. □

THEOREM 5. *Let K be an axiomatizable class of algebraic systems of a signature Σ.*

(a) *K is $\exists$-axiomatizable $\Leftrightarrow$ K is closed under supersystems.*

(b) *K is $\forall$-axiomatizable $\Leftrightarrow$ K is closed under subsystems.*

PROOF. The statements $\Rightarrow$ follow from Proposition 4.

(a) We first show that for any sentence $\Phi \in \mathrm{Th}(K)$ there is a sentence $\Psi_\Phi \in \mathrm{Th}(K)$ such that $\rhd \Psi_\Phi \to \Phi$ and for any pair $\mathfrak{A} \subseteq \mathfrak{B}$ of algebraic systems of Σ $\mathfrak{A} \models \Psi_\Phi$ implies $\mathfrak{B} \models \Phi$. Suppose that this is not the case, i. e. that there is $\Phi_0 \in \mathrm{Th}(K)$ such that for any $\Psi \in \mathrm{Th}(K)$ there are systems $\mathfrak{A}_\Psi \subseteq \mathfrak{B}_\Psi$ of Σ for which $\rhd \Psi \to \Phi_0$ yields $\mathfrak{A}_\Psi \models \Psi$ and $\mathfrak{B}_\Psi \models \neg \Phi_0$. Let D be an ultrafilter on the set $\mathrm{Th}(K)$ containing a family of sets with finite intersection property $X = \{u_\Phi \mid \Phi \in \mathrm{Th}(K)\}$, where $u_\Phi = \{\Psi \in \mathrm{Th}(K) \mid \rhd \Psi \to \Phi\}$. Consider systems $\mathfrak{A}_0 = D\text{-prod}\, \mathfrak{A}_\Psi$ and $\mathfrak{B}_0 = D\text{-prod}\, \mathfrak{B}_\Psi$. Since $\mathfrak{A}_\Psi \subseteq \mathfrak{B}_\Psi$ for all $\Psi \in \mathrm{Th}(K)$, there is $\mathfrak{A}_1 \subseteq \mathfrak{B}_0$, $\mathfrak{A}_1 \simeq \mathfrak{A}_0$. From Theorem 17.1, the inclusion $X \subseteq D$ and from the fact that $\mathfrak{A}_0 \simeq \mathfrak{A}_1$ we get $\mathfrak{A}_1 \in K_\Sigma(\mathrm{Th}(K)) = K$ and $\mathfrak{B}_0 \models \neg \Phi_0$. This contradicts the fact that K is closed under supersystems.

---

* Recall that the elements of Γ are sentences and hence are not affected by the replacement.

For any sentence $\Phi \in \mathrm{Th}(K)$ there is by Lemma 1 (set $\Gamma = \{\Psi_\Phi \vee \neg \Phi\}$ and $\Psi_0 = \Phi$) an $\exists$-sentence X_Φ such that $\rhd \Psi_\Phi \vee \neg \Phi \rightarrow ((\Phi \rightarrow X_\Phi) \wedge (X_\Phi \rightarrow \Phi))$. It follows that $X_\Phi \rightarrow \Phi$ is an identically true sentence and by virtue of $\{\Phi, \Psi_\Phi\} \subseteq \mathrm{Th}(K)$ also $X_\Phi \in \mathrm{Th}(K)$. Hence the set of $\exists$-sentences $\{X_\Phi \mid \Phi \in \mathrm{Th}(K)\}$ is an axiom system for K.

(b) To prove (b) it is necessary to replace in the proof of (a) $\mathfrak{A} \subseteq \mathfrak{B}$ and $\mathfrak{A}_\Psi \subseteq \mathfrak{B}_\Psi$ by $\mathfrak{B} \subseteq \mathfrak{A}$ and $\mathfrak{B}_\Psi \subseteq \mathfrak{A}_\Psi$ respectively and apply the other part of Lemma 1.

DEFINITION. A sentence of the form $\forall x_1 \ldots \forall x_k Q$, where Q is an atomic formula, is called an *identity*. A sentence of the form

$$\forall x_1 \ldots \forall x_k (Q_1 \wedge \ldots \wedge Q_n \rightarrow Q_0), \tag{1}$$

where $Q_0, Q_1, \ldots, Q_n$ are atomic formulas, is a *quasi-identity*. An axiomatizable class K is said to be a *variety* (*quasi-variety*) if there is an axiom system Z for K consisting of *identities* (*quasi-identities*).

Since an identity $\forall x_1 \ldots \forall x_k Q$ is equivalent to an identity $\forall x_1 \ldots \forall x_{k+1} (x_{k+1} \approx x_{k+1} \rightarrow Q)$, a variety is a quasi-variety.

A system $E_\Sigma = \langle \{\varnothing\}, \nu^{E_\Sigma} \rangle$ is said to be a *unit system of a signature* Σ if

$$\nu^{E_\Sigma}(s) = \{\varnothing\}^{\mu(s)} \quad \text{for all} \quad s \in R. \tag{2}$$

Condition (2) defines E_Σ uniquely since for any $n \in \omega$ on a one-element set there is only one n-place function.

PROPOSITION 5. (a) *Any quasi-variety K of a signature Σ is closed under filtered products and contains a unit system E_Σ.*

(b) *Any variety is closed under homomorphic images.*

PROOF. (a) Since $Q_0(\varnothing, \ldots, \varnothing)$ is true in E_Σ for any atomic formula $Q_0(x_1, \ldots, x_n)$ of Σ, any quasi-identity (1) is true in E_Σ. To show that K is closed under filtered products it suffices to establish that any quasi-identity (1) conditionally filters for any filter D on a set I. By Lemma 17.2 it suffices to establish that a formula $(Q_1 \wedge \ldots \wedge Q_n \to Q_0)(x_1, \ldots, x_k)$ conditionally filters for D. Let $f_1, \ldots, f_k \in I$-prod A_i and $X = \{i \mid \mathfrak{A}_i \models (Q_1, \ldots, Q_n \to Q_0)(f_1 i, \ldots, f_k i)\} \in D$. Suppose that $(Q_1 \wedge \ldots \wedge Q_n \wedge \neg Q_0)(Df_1, \ldots, Df_k)$ is true in D-prod $\mathfrak{A}_i$. From Lemmas 17.3 and 17.2 we get $Y = \{i \mid \mathfrak{A}_i \models (Q_1 \wedge \ldots \wedge Q_n)(f_1 i, \ldots, f_k i) \in D$ and $Z = \{i \mid \mathfrak{A}_i = Q_0(f_1 i, \ldots, f_k i)\} \notin D$. It is obvious that $X \cap Y$ is contained in Z. Since $X \cap Y \in D$, we have $Z \in D$, a contradiction.

(b) Let f be a homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$. By Proposition 16.1 (b) for any term t and any interpretation $\gamma\colon FV(t) \to A$

$$f(t^{\mathfrak{A}}[\gamma]) = t^{\mathfrak{B}}[\gamma f].$$

From this equation and the definition of a homomorphism we get

$$\mathfrak{A} \models Q[\gamma] \Rightarrow \mathfrak{B} \models Q[\gamma f]$$

for any atomic formula Q of Σ. By virtue of the fact that f maps A onto B therefore if any identity Φ is true in $\mathfrak{A}$ it is true in $\mathfrak{B}$. □

THEOREM 6. *For an* $\forall$*-axiomatizable class* K *of a signature* Σ *the following conditions are equivalent*:

(a) K *is a quasi-variety*,

(b) K *is closed under finite Cartesian products and contains a unit system* E_Σ.

PROOF. (a) $\Rightarrow$ (b) is proved in Proposition 5 (a). Consider a set

$$W = \{\Phi \mid \Phi \text{ is a quasi-identity of } \Sigma \text{ and } \Phi \in \mathrm{Th}(K)\}.$$

Let $\mathfrak{A}$ be a model of W. We show that every finite subset $X \subseteq D(\mathfrak{A})$ has a model $\mathfrak{B}_X$ such that $\mathfrak{B}_X \restriction \Sigma \in K$. Let $X = Y \cup Z$, where Z consists of atomical sentences and Y consists of negations of atomical sentences. If $Y = \varnothing$, then one may take E_{Σ_A} as $\mathfrak{B}_X$. Let $Y = \{\neg Q_1, \ldots, \neg Q_n\}$ and suppose Φ is a conjunction of elements of Z if $Z = \varnothing$ and Φ is $c_a \approx c_a$ for some $a \in A$ if $Z = \varnothing$. Let $c_{a_1}, \ldots, c_{a_k}$ be all constants of C_A occurring in $Q_1, \ldots, Q_n, \Phi$ and let $Q_1', \ldots, Q_n', \Phi'$ be obtained from $Q_1, \ldots, Q_n, \Phi$ by replacing $c_{a_1}, \ldots, c_{a_k}$ by $x_1, \ldots, x_k$ respectively. Since quasi-identities $\forall x_1 \ldots \forall x_k Q(\Phi \to Q_i)$, $1 \leqslant i \leqslant n$, are false in $\mathfrak{A}$, they are not in W. Hence there are systems $\mathfrak{B}_1, \ldots, \mathfrak{B}_n \in K$ such that $\mathfrak{B}_i \models (\Phi \wedge \neg Q_i)[\gamma_i]$, $1 \leqslant i \leqslant n$, for some $\gamma_i\colon \{x_1, \ldots, x_k\} \to B_i$. Consider a Cartesian product $\mathfrak{B}_1 \times \ldots \times \mathfrak{B}_n \in K$ and an interpretation

γ of variables $x_1, \ldots, x_k$ in B for which the projection $i(\gamma)$ on the ith coordinate is γ_i. From Lemma 17.3 we get $\mathfrak{B}_1 \times \ldots \times \mathfrak{B}_n \models (\Phi \wedge \neg Q_1 \wedge \ldots \wedge \neg Q_n)[\gamma]$. Hence the system $\mathfrak{B}_1 \times \ldots \times \mathfrak{B}_n$ can be expanded to a system $\mathfrak{B}_X$ of Σ_A which is a model of X. It follows from the proof of Theorem 17.2 that there is an ultraproduct $\mathfrak{B} = D\text{-prod}\ \mathfrak{B}_X$ which is a model of $D(\mathfrak{A})$. By Proposition 24.4 (a) there is a subsystem $\mathfrak{B}_1 \subseteq \mathfrak{B} \upharpoonright \Sigma$ such that $\mathfrak{A} \simeq \mathfrak{B}_1$. Since $\mathfrak{B} \upharpoonright \Sigma = D\text{-prod}\,(\mathfrak{B}_X \upharpoonright \Sigma)$ and $\mathfrak{B}_X \upharpoonright \Sigma \in K$, it follows from Theorems 4 and 5 and from the fact that $\mathfrak{A} \simeq \mathfrak{B}_1$ that $\mathfrak{A} \in K$. Thus we have $K = K_\Sigma(W)$. □

THEOREM 7. *For a quasi-variety K of a signature Σ the following conditions are equivalent*:

(a) *K is a variety*,

(b) *K is closed under homomorphic images.*

PROOF. (a) ⇒ (b) is shown in Proposition 5 (b). Suppose (b) holds and $\mathfrak{A}$ is a model of a set

$$Z = \{\Phi \mid \Phi \text{ is an identity of } \Sigma \text{ and } \Phi \in \mathrm{Th}(K)\}.$$

Consider a set

$$D^-(\mathfrak{A}) = \{\Phi \in D(\mathfrak{A}) \mid \Phi \text{ contains a negation}\}.$$

For any formula $\neg\Psi$ in $D^-(\mathfrak{A})$ an identity $\forall y_1, \ldots \forall y_n \Psi_1$ of Σ, where $\Psi = (\Psi_1)^{y_1, \ldots, y_n}_{c_{a_1}, \ldots, c_{a_n}}$, is false in $\mathfrak{A}$ and so it is not in Z. Hence there is $\mathfrak{B}_\Psi \in K$ and an interpretation $\gamma_\Psi\colon \{y_1, \ldots, y_n\} \to B_\Psi$ for which $\mathfrak{B}_\Psi \models \neg\Psi_1[\gamma_\Psi]$. Therefore $\mathfrak{B}_\Psi$ can be expanded to a system $\mathfrak{B}'_\Psi$ of Σ_A which is a model of $\{\neg\Psi\}$. Consider a Cartesian product $\mathfrak{B} = D^-(\mathfrak{A})\text{-prod}\ \mathfrak{B}_\Psi$. By Proposition 5 (a) we have $\mathfrak{B} \upharpoonright \Sigma \in K$. By Lemma 17.3 $\mathfrak{B} \models \neg\Psi$ for any $\neg\Psi \in D^-(\mathfrak{A})$. Let $\mathfrak{B}_1$ be a subsystem of $\mathfrak{B}$ generated in $\mathfrak{B}$ by a set $\{\nu^{\mathfrak{B}}(c_a) \mid a \in A\}$. By Theorem 5 (b) we have $\mathfrak{B}_1 \upharpoonright \Sigma \in K$. We define a mapping $h\colon B_1 \to A$ as follows: if $t(x_1, \ldots, x_m)$ is a term of Σ and $t^{\mathfrak{B}}(\nu^{\mathfrak{B}}(c_{a_1}), \ldots, \nu^{\mathfrak{B}}(c_{a_m})) = b$, then $h(b) = t^{\mathfrak{A}}(a_1, \ldots, a_m)$. The correctness of the definition of h follows from implications:

$$\mathfrak{B}_1 \models (t_1 \approx t_2)(\nu^{\mathfrak{B}}(c_{a_1}), \ldots, \nu^{\mathfrak{B}}(c_{a_m})) \Rightarrow$$
$$\Rightarrow (\neg t_1 \approx t_2)^{x_1, \ldots, x_m}_{c_{a_1}, \ldots, c_{a_m}} \notin D^-(\mathfrak{A}) \Rightarrow \mathfrak{A} \models (t_1 \approx t_2)(a_1, \ldots, a_m),$$

where $t_1(x_1, \ldots, x_m)$ and $t_2(x_1, \ldots, x_m)$ are any terms of Σ. The chain of implications which is obtained from the previous one by replacing $t_1 \approx t_2$ by any atomical formula $Q(x_1, \ldots, x_m)$ of Σ also holds and so h is a homomorphism of $\mathfrak{B}_1$ onto $\mathfrak{A}$. From (b) we get $\mathfrak{A} \in K$. It is thus shown that $K = K_\Sigma(Z)$. □

Exercises

1. Let K be an axiomatizable class containing systems of arbitrarily large finite powers. Show that a class K_∞ consisting of infinite systems of the class K is axiomatizable but is not finitely axiomatizable.

2. Show that in Theorem 4 the condition of closure under an elementary equivalence may be replaced by closure under isomorphisms and elementary subsystems. (*Hint*. Consider $D^*(\mathfrak{A})$ instead of $\mathrm{Th}(\mathfrak{A})$ in the proof of Theorem 4.)

3. Show that any quasi-identity Φ is equivalent to a quasi-identity Ψ in reduced nf.

4. No statement similar to that of Exercise 3 holds for identities. Find a variety that has no axiom system consisting of sentences of the form $\forall x_1 \ldots \forall x_n Q$, where Q is an atomical formula. (*Hint*. Consider a variety with an axiom system $\{\forall x P(f(x))\}$.)

26. SKOLEM FUNCTIONS

DEFINITION. A set T of sentences of a signature Σ closed under derivability (i. e. if $T \rhd \Phi$ and Φ is a sentence of Σ, then $\Phi \in T$) is called an *elementary theory*, or simply a *theory of the signature* Σ. A consistent theory T of Σ is said to be *complete* if $\Phi \in T$ or $\neg \Phi \in T$ for any sentence Φ of Σ. A consistent theory T of Σ is said to be *model-complete* if $\mathfrak{A} \subseteq \mathfrak{B} \Rightarrow \mathfrak{A} \prec \mathfrak{B}$ for any models $\mathfrak{A}$, $\mathfrak{B}$ of T having the signature Σ. Formulas Φ and Ψ of Σ are said to be *equivalent with respect to* a theory T of Σ (we write $\Phi \overset{T}{\equiv} \Psi$) if $T \rhd (\Phi \to \Psi) \wedge (\Psi \to \Phi)$. A theory T of Σ is said to be *$\forall$-axiomatizable* or *universally axiomatizable* (*$\exists$-axiomatizable*, *$\forall\exists$-axiomatizable*) if there is a set $Z \subseteq T$ of $\forall$-sentences ($\exists$-sentences, $\forall\exists$-sentences) such that $Z \rhd \Phi$ for any $\Phi \in T$. Such a set Z is called an *axiom system for the theory* T.

It follows from Corollary 22.4 that a theory T of a signature Σ is $\forall$-axiomatizable ($\exists$-axiomatizable, $\forall\exists$-axiomatizable) exactly when the class $K = K_\Sigma(T)$ is $\forall$-axiomatizable ($\exists$-axiomatizable, $\forall\exists$-axiomatizable), with Z being an axiom system for T if Z is an axiom system for $K_\Sigma(T)$ and vice versa.

A theory T of Σ is said to be a *theory with elimination of quantifiers* if any formula Φ of Σ is equivalent with respect to T to some quantifier-free formula Ψ. It is obvious that a consistent theory with elimination of quantifiers is model-complete. On the other hand, a model-complete theory T is "almost" a theory with elimination of quantifiers. Namely, we have the following

THEOREM 8. *For a consistent theory T of a signature Σ to be model-complete it is necessary and sufficient that any formula Φ of Σ should be equivalent with respect to T to some $\forall$-formula X_1 and to some $\exists$-formula X_2.*

PROOF. Sufficiency follows from Proposition 25.4 (a). Necessity is obtained from Lemma 25.1 by taking as Γ a theory T. □

The requirement in Theorem 8 that Φ should be equivalent to some $\exists$-formula X_2 may be omitted, of course, since this follows from the equivalence of $\neg\Psi$ to some $\forall$-formula.

To work with formulas containing quantifiers is much more difficult than with quantifier-free formulas. Therefore theorems of model theory of the form: a given theory T is a theory with elimination of quantifiers (is model-complete), are very important. We shall now present a certain construction, first proposed by Skolem, that allows any theory to be extended to an $\forall$-axiomatizable model-complete theory.

DEFINITION. If Σ is a signature, then a signature Σ^S is obtained from Σ by adding new n-place function symbols f_Φ for every formula $\Phi = \exists x\Psi$ of Σ that begins with an existential quantifier and has n free variables. By S we denote a set of sentences

$$\forall x_1 \dots \forall x_n(\Phi(x_1, \dots, x_n) \to \Psi(f_\Phi(x_1, \dots, x_n), x_1, \dots, x_n))$$

for all formulas $\Phi(x_1, \dots, x_n) = \exists x\Psi(x, x_1, \dots, x_n)$ of Σ with free variables $x_1, \dots, x_n$ written out in the order of their first free occurrences in the formula Φ. If T is a theory of Σ, then by T^S we denote a theory

$$\{\Phi \mid \Phi \text{ is a sentence of a signature } \Sigma^S \text{ and } T \cup S \rhd \Phi\}.$$

The signature Σ^S (the theory T^S) is a *skolemization of the signature* Σ (of the theory T). A model $\mathfrak{A}^S$ of the theory $(\mathrm{Th}(\mathfrak{A})^S)$ having a signature Σ^S is called a *skolemization of a system* $\mathfrak{A}$ of Σ if $\mathfrak{A}^S \restriction \Sigma = \mathfrak{A}$.

Unlike Σ^S and T^S a skolemization $\mathfrak{A}^S$ is not uniquely defined by $\mathfrak{A}$, two skolemizations of $\mathfrak{A}$ may not even be elementarily equivalent (see Exercise 1). Moreover, it follows from Exercise 1 that T^S is almost always incomplete.

PROPOSITION 1. (a) *Let T be a theory of a signature Σ, $\mathfrak{B}$ be a model of the theory T^S and $\mathfrak{A} \subseteq \mathfrak{B}$. Then $\mathfrak{A} \restriction \Sigma \prec \mathfrak{B} \restriction \Sigma$.*

(b) *Any algebraic system $\mathfrak{A}$ has some skolemization $\mathfrak{A}^S$.*

PROOF. (a) Follows immediately from Proposition 24.1. We prove (b). If $\Phi = \exists x \Psi(x, x_1, \ldots, x_n)$, then for $a_1, \ldots, a_n \in A$ we take as a value of $\nu^{\mathfrak{A}}(f_\Phi)(a_1, \ldots, a_n)$ an element $a_0 \in A$ for which $\mathfrak{A} \models \Psi(a_0, a_1, \ldots, a_n)$, if there is such an element $a_0 \in A$, and an arbitrary element $a \in A$, if there is no such element a_0. □

From Proposition 1 we at once obtain Theorem 2 of Sec. 24. In that theorem as $\mathfrak{B}$ it is sufficient to take $\mathfrak{B}_1 \restriction \Sigma$, where $\mathfrak{B}_1$ is a subsystem of $\mathfrak{A}^S$ generated by the set X.

Skolemization allows one to "remove" quantifiers from the formulas of an old signature Σ. They "remain", however, in the formulas of the new signature, Σ^S. To avoid this inconvenience we "close" the skolemization process.

DEFINITION. Let Σ be a signature and let T be a theory of Σ. We define signatures Σ^{ns} and theories T^{ns}, $n \in \omega$, by induction: $\Sigma^{0s} = \Sigma$, $T^{0s} = T$, $\Sigma^{(n+1)s} = (\Sigma^{ns})^s$, $T^{(n+1)s} = (T^{ns})^s$. A signature $\Sigma^{cs} = \bigcup_{n \in \omega} \Sigma^{ns}$ (a theory $T^{cs} = \bigcup_{n \in \omega} T^{ns}$) is called the *complete skolemization of the signature Σ (the theory T)*. An algebraic system $\mathfrak{A}^{cs}$ of the signature Σ^{cs} is said to be a *complete skolemization of a system* $\mathfrak{A}$ of Σ if $\mathfrak{A}^{cs} \restriction \Sigma = \mathfrak{A}$ and $\mathfrak{A}^{cs}$ is a model of $(\mathrm{Th}(\mathfrak{A}))^{cs}$.

PROPOSITION 2. (a) *Any algebraic system $\mathfrak{A}$ has some complete skolemization $\mathfrak{A}^{cs}$.*

(b) *Let T be a consistent theory of a signature Σ. Then a theory T^{cs} is a universally axiomatizable model-complete extension of T and for any model $\mathfrak{A}$ of T there is a model $\mathfrak{A}_1$ of T^{cs} such that $\mathfrak{A} \restriction \Sigma = \mathfrak{A}$.*

PROOF. (a) By Proposition 1 (b) there are systems $\mathfrak{A}^{ns}$, $n \in \omega$, such that $\mathfrak{A}^{0s} = \mathfrak{A}$ and $\mathfrak{A}^{(n+1)s}$ is a skolemization of $\mathfrak{A}^{ns}$. Let $\mathfrak{A}^{ns} = \langle A, \nu^{\mathfrak{A}^{cs}} \rangle$ be a system of the signature Σ^{cs} where $\nu^{\mathfrak{A}^{cs}}$ coincides with $\nu^{\mathfrak{A}^{ns}}$ on the symbols of Σ^{ns}. It is clear that $\mathfrak{A}^{cs}$ is a complete skolemization of $\mathfrak{A}$.

(b) Let $\mathfrak{A}$ be a model of T^{cs} of a signature Σ^{cs} and $\mathfrak{B} \subseteq \mathfrak{A}$. From Proposition 1 (a) we get $\mathfrak{B} \upharpoonright \Sigma^{ns} \prec \mathfrak{A} \upharpoonright \Sigma^{ns}$ for any $n \in \omega$. Since $\Sigma^{cs} = \bigcup\limits_{n \in \omega} \Sigma^{ns}$, we get $\mathfrak{B} \prec \mathfrak{A}$. Hence T^{cs} is model-complete and by Theorem 5 the class $K_{\Sigma^{cs}}(T^{cs})$ is $\forall$-axiomatizable, i. e. $K_{\Sigma^{cs}}(T^{cs}) = K_{\Sigma^{cs}}(Z)$, where Z is a set of $\forall$-sentences of Σ^{cs}. Then Z is an axiom system for T^{cs}. The second statement in (b) follows from (a). ☐

Exercise

1. Show that for all skolemizations of a system $\mathfrak{A}$ to be elementarily equivalent it is necessary and sufficient that A be one-element. (*Hint*. Consider different values of $\nu^{\mathfrak{A}^S}(f_\Phi)$ for $\Phi = \exists v_0(v_0 \approx v_0 \wedge v_1 \approx v_1)$.)

27. MECHANISM OF COMPATIBILITY

The mechanism of compatibility is mainly of methodical importance. It allows us to recognize a common part in many theorems proving which involves construction of models. In this section we prove several such theorems. It is assumed throughout that the signature Σ has a finite or countable power.

DEFINITION. For a formula Φ of Σ we define a formula $\Phi\neg$ as follows:

(a) if Φ is an atomic formula, then $\Phi\neg = \neg\Phi$,
(b) $(\neg\Psi)\neg = \Psi$,
(c) $(\Psi_1 \to \Psi_2)\neg = \Psi_1 \wedge \neg\Psi_2$,
(d) $(\Psi_1 \wedge \Psi_2)\neg = \neg\Psi_1 \vee \neg\Psi_2$,
(e) $(\Psi_1 \vee \Psi_2)\neg = \neg\Psi_1 \wedge \neg\Psi_2$,
(f) $(\exists x\Psi)\neg = \forall x\neg\Psi$,
(g) $(\forall x\Psi)\neg = \exists x\neg\Psi$.

It is seen from the definition of $\Phi\neg$ that $\Phi\neg \equiv \neg\Phi$. We denote by Σ^c a signature obtained from a signature $\Sigma = \langle R, F, \mu\rangle$ by adding to it a countable set C of new constants. A constant of Σ^c and a term of the form $f(c_1, \ldots, c_n)$, where $c_1, \ldots, c_n \in C$ and $f \in F$, will be called a *basis term of the signature* Σ^c.

DEFINITION. A set S of finite or countable sets of sentences of Σ^c is said to be the *mechanism of compatibility of a signature* Σ if for each $s \in S$ the following conditions hold:

(C1) the inclusion $\{\Phi, \neg\Phi\} \subseteq s$ holds for no sentence Φ;

(C2) $\neg\Phi \in s \Rightarrow (s \cup \{\Phi\neg\} \subseteq s_1$ for some $s_1 \in S)$;

(C3) $\Phi \rightarrow \Psi \in s \Rightarrow (s \cup \{\Psi\} \subseteq s_1$ or $s \cup \{\neg\Phi\} \subseteq s_1$ for some $s_1 \in S)$;

(C4) $\Phi \wedge \Psi \in s \Rightarrow (s \cup \{\Phi\} \subseteq s_1$ and $s \cup \{\Psi\} \subseteq s_2$ for some $s_1, s_2 \in S)$;

(C5) $\Phi \vee \Psi \in s \Rightarrow (s \cup \{\Phi\} \subseteq s_1$ or $s \cup \{\Psi\} \subseteq s_1$ for some $s_1 \in S)$;

(C6) $\forall x\Phi \in s \Rightarrow$ (for any $c \in C$ there is $s_1 \in S$ such that $s \cup \cup \{(\Phi)^x_c\} \subseteq s_1)$;

(C7) $\exists x\Phi \in s \Rightarrow (s \cup \{(\Phi)^x_c\} \subseteq s_1$ for some $c \in C$ and some $s_1 \in \in S)$;

(C8) $(c_1, c_2 \in C$ and $c_1 \approx c_2 \in s) \Rightarrow (s \cup \{c_2 \approx c_1\} \subseteq s_1$ for some $s_1 \in S)$;

(C9) if $c \in C$ and t is a basis term of Σ^c, then two conditions hold:

(a) $s \cup \{d \approx t\} \subseteq s_1$ for some $d \in C$ and some $s_1 \in S$,

(b) $\{c \approx t, (\Phi)^x_t\} \subseteq s \Rightarrow (s \cup \{(\Phi)^x_c\} \subseteq s_1$ for some $s_1 \in S)$.

A set S is said to be a *mechanism of compatibility* if it is the mechanism of compatibility of some signature Σ.

PROPOSITION 1. *Let T be a theory of a signature Σ. Then a set S of finite sets s of sentences of a signature Σ^c such that $T \cup s$ is compatible is a mechanism of compatibility.*

PROOF. We verify condition (C7). Checking the remaining conditions will be left as an easy exercise to the reader. Let a set $T \cup \cup s \cup \{(\Phi)^x_c\}$ be incompatible for a constant $c \in C$ not occurring in the elements of $s \cup \{\Phi\}$ and let D be a proof of a sequent $\Psi_1, \ldots, \Psi_n, (\Phi)^x_c \vdash$, where $\{\Psi_1, \ldots, \Psi_n\} \subseteq T \cup s$. We employ the usual device: by replacing the constant c in all the sequents of D by a variable y not occurring in the elements of D we obtain a proof D_1 of the sequent $\Psi_1, \ldots, \Psi_n, (\Phi)^x_y \vdash$. Applying Rule 16 we obtain the provability of $\Psi_1, \ldots, \Psi_n, \exists y(\Phi)^x_y \vdash$. Since $\exists x\Phi$ and $\exists y(\Phi)^x_y$ are congruent, the set $T \cup s$ is incompatible if $\exists x\Phi \in s$. ☐

PROPOSITION 2. *Let S be a mechanism of compatibility and $s \in S$.*

(a) $\{\Phi, \Phi \rightarrow \Psi\} \subseteq s \Rightarrow (s \cup \{\Psi\} \subseteq s_1$ for some $s_1 \in S)$.

(b) *For any* $c \in C$ *there is* $s_1 \in S$ *such that* $s \cup \{c \approx c\} \subseteq s_1$.

(c) $(c, d, e \in C$ *and* $\{c \approx d, d \approx e\} \subseteq s) \Rightarrow (s \cup \{c \approx e\} \subseteq s_1$ *for some* $s_1 \in S)$.

(d) $S' = \{s' \mid s' \subseteq s \in S\}$ *is a mechanism of compatibility.*

PROOF. (d) Is obvious, (a) follows from (C3) and (C1), (c) follows from (C9) (b) if we take $x \approx e$ as Φ and a constant d as t. We prove (b). By (C9) (a) we have $s \cup \{d \approx c\} \subseteq s_1$ for some constant $d \in C$ and $s_1 \in S$. From (C8) we get $s \cup \{d \approx c, c \approx \approx d\} \subseteq s_1$ for some $s_1 \in S$. Now we apply (c) and get $s \cup \{d \approx c, c \approx d, c \approx c\} \subseteq s_1$ for some $s_1 \in S$. □

An algebraic system $\mathfrak{A}$ of Σ^c is said to be *canonical* if $\nu^{\mathfrak{A}}(C) = A$, i. e. any element $a \in A$ is the value of some constant $c \in C$.

THEOREM 9. If S is a mechanism of compatibility of a signature Σ and $s^* \in S$, then s^* has a canonical model $\mathfrak{A}$ of a signature Σ^c.

PROOF. Consider a class $S' = \{s' \subseteq s \mid s \in S\}$, which is by Proposition 2 (d) a mechanism of compatibility. Let

$$\Phi_0, \quad \Phi_1, \ldots, \Phi_n, \ldots \qquad (n \in \omega)$$

be an enumeration of all sentences of Σ^c and let

$$t_0, t_1, \ldots, t_n, \ldots \qquad (n \in \omega)$$

be an enumeration of all basis terms of Σ^c. By induction on $n \in \omega$ we construct a sequence

$$s_0 \subseteq s_1 \subseteq \ldots \subseteq s_n \subseteq \ldots$$

of the elements of S'. We set $s_0 = s^*$. If $n = 3k$, then by (C9) (a) we find a constant $c \in C$ such that $s_n \cup \{c \approx t_k\} \in S'$ and set $s_{n+1} = s_n \cup \{c \approx t_k\}$. For $n = 3k + 1$ we set $s_{n+1} = s_n \cup \cup \{\Phi_k\}$, if $s_n \cup \{\Phi_k\} \in S'$ and $s_{n+1} = s_n$ otherwise. Let $n = = 3k + 2$. If $\Phi_k = \exists x \Psi$ and $\Phi_k \in s_n$, then we set $s_{n+1} = s_n \cup \cup \{(\Psi)^x_c\} \in S'$ for some $c \in C$. Otherwise we set $s_{n+1} = s_n$. Consider a set $s_\omega = \bigcup\limits_{n \in \omega} s_n$. The construction of s_ω implies the following fact:

(∗) a one-element set $\{s_\omega\}$ is a mechanism of compatibility.

On the set C we define the relation $\sim$:

$$c \sim d \Leftrightarrow c \approx d \in s_\omega .$$

By (C8) and Proposition 2 (b), (c) the relation $\sim$ is an equivalence on the set C. On the set $A = \{\tilde{c} \mid \tilde{c}$ is a $\sim$-equivalence class containing $c \in C\}$ we define an interpretation $\nu^{\mathfrak{A}}$ of a signature $\Sigma^c = \langle R, F^c, \mu^c \rangle$ as follows:

$$\nu^{\mathfrak{A}}(f)(\tilde{c}_1, \ldots, \tilde{c}_n) = \tilde{c} \Leftrightarrow c \approx f(c_1, \ldots, c_n) \in s_\omega,$$

$$\langle \tilde{c}_1, \ldots, \tilde{c}_n \rangle \in \nu^{\mathfrak{A}}(r) \Leftrightarrow r(c_1, \ldots, c_n) \in s_\omega,$$

where $f \in F^c$, $r \in R$, $\mu^c(f) = \mu^c(r) = n$. It follows from $(*)$ and (C9) (b) that these definitions are correct. Suppose, for example, that $c_1 \approx f(c_2, c_3)$, $c_4 \approx f(c_5, c_6)$, $c_2 \approx c_5$ and $c_3 \approx c_6$ are in s_ω. Applying $(*)$ and (C9) (b) yields $c_4 \approx f(c_2, c_6) \in s_\omega$. Applying two more times $(*)$ and (C9) (b) yields $c_4 \approx f(c_2, c_3) \in s_\omega$ and $c_4 \approx c_1 \in s_\omega$.

Since $\nu^{\mathfrak{A}}(c) = \tilde{c}$ for $\tilde{c} \in C$, we set that $\mathfrak{A} = \langle A, \nu^{\mathfrak{A}} \rangle$ is a canonical system. We now show that for any sentence Φ of Σ^c

$$\Phi \in s_\omega \Rightarrow \mathfrak{A} \models \Phi. \tag{1}$$

It follows that $\mathfrak{A}$ is a model of s^*. If $\Phi = c \approx t$ for a basis term t, $c \in C$, $\Phi = r(c_1, \ldots, c_n)$ for $r \in R$, $c_1, \ldots, c_n \in C$, or Φ is the negation of such formulas, then (1) follows from the definition of $\nu^{\mathfrak{A}}$, $(*)$ and (C1). If $t \approx c \in s_\omega$, where t is a basis term, $c \in C$, then from $(*)$ and (C9) (b) we get $d \approx t \in s_\omega$ for some $d \in C$. Therefore by $(*)$ and (C9) (b) we have $d \approx c \in s_\omega$. Hence $\mathfrak{A} \models t \approx c$. Let $\neg t \approx c \in s_\omega$, where t is a basis term, $c \in C$. If $\neg t \approx c$ is false in $\mathfrak{A}$, then by the definition of $\mathfrak{A}$ $c \approx t \in s_\omega$. From $(*)$ and (C9) (b) we get $\neg c \approx c \in s_\omega$. By virtue of $(*)$ and Proposition 2 (b) this contradicts (C1). We have thus shown that (1) is true if Φ is an atomic sentence or the negation of an atomic sentence and the number $n(\Phi)$ of the symbols of Σ occurring in Φ is not greater than 1. Let $\Phi \in s_\omega$ be an atomic sentence or the negation of an atomic sentence and $n(\Phi) > 1$. Then there is a basis term $t \notin C$ occurring in Φ. By properties $(*)$ and (C9) (a) we have $d \approx t \in s_\omega$ for some $d \in C$. It follows from $(*)$ and (C9) (b) that the formula Φ_1 obtained from Φ by replacing t by d is in s_ω. Since $n(\Phi_1) < n(\Phi)$, by the induction hypothesis Φ is true in $\mathfrak{A}$. For the remaining sentences Φ of Σ^c statement (1) is obtained immediately from $(*)$ and (C2) to (C7) by induction on the length of Φ. □

DEFINITION. A set S of finite or countable sets of sentences of a signature Σ^c is said to be a *mechanism of compatibility of a signature* Σ *without equality* if S satisfies conditions (C1) to (C7) and the sentences occurring in the elements of S do not contain an equality.

THEOREM 9′. *If a signature* Σ *contains no function and constant symbols and* S *is a mechanism of compatibility of* Σ *without equality, then any* $s^* \in S$ *has a canonical model of a signature* Σ^c.

PROOF. Consider a set $X = \{c \approx c \mid c \in C\}$ and a class $S' = \{s \cup X \mid s \in S\}$. It is obvious that S' is a mechanism of compatibility of Σ. By Theorem 9 $s^* \cup X$ has a canonical model of Σ^c. □

The following theorem is a generalization of Theorem 9 which we shall need in what follows.

THEOREM 10. *Let* S *be a mechanism of compatibility of a signature* Σ, X_i, $i \in \omega$, *be finite or countable sets of sentences of a signature* Σ^c *and let* T *be a consistent theory of* Σ. *Suppose that for any* $s \in S$, $\Phi \in T$ *and* $i \in \omega$ *there are* $\Psi \in X_i$ *and* $s_1 \in S$ *such that* $s \cup \{\Phi, \Psi\} \subseteq s_1$. *Then for any* $s^* \in S$ *there is a set* X *of sentences of* Σ *such that* $s^* \cup X \cup T$ *has a canonical model* $\mathfrak{A}$ *and* $X \cap X_i \neq \varnothing$ *for any* $i \in \omega$.

PROOF. Consider a class $S' = \{s \cup T \mid s \in S\}$. It is easily verified that S' is a mechanism of compatibility. For example, let $\exists x\Phi \in s \cup T$ and $s \in S$. If $\exists x\Phi \in s$, then by (C7) $s \cup \{(\Phi)^x_c\} \cup T \subseteq s_1 \cup T$ for some $s_1 \in S$. If $\exists x\Phi \in T$, then under the hypothesis of the theorem there is $s_1 \in S$ such that $s \cup \{\exists x\Phi\} \subseteq s_1$. Again by (C7) we have $s_1 \cup \{(\Phi)^x_c\} \subseteq s_2$ for some $c \in C$ and $s_2 \in S$. Hence $s \cup T \cup \{(\Phi)^x_c\} \subseteq s_2 \cup T$. Let $\Phi_0, \Phi_1, \ldots, \Phi_n, \ldots$ $(n \in \omega)$ and $t_0, t_1, \ldots, t_n, \ldots$ $(n \in \omega)$ be enumerations of all sentences of the signature Σ^c and of all basis terms of Σ^c.

From S' we construct a set $s_\omega = \bigcup_{n \in \omega} s_n$ as follows. The set s_0 is equal to $s^* \cup T$, and we determine s_{n+1} for n equal to $4k$, $4k + 1$ or $4k + 2$ from S' in the same way as s_{n+1} for n equal to $3k$, $3k + 1$ or $3k + 2$ respectively are constructed from S in Theorem 9. For $n = 4k + 3$ we proceed as follows: if $s_n = s'_n \cup T$, $s'_n \in S$, then under the hypothesis of the theorem there are $\Psi \in X_k$ and $s' \in S$ such that $s'_n \cup \{\Psi\} \subseteq s'$; we set $s_{n+1} = s' \cup T$. The construction of the model $\mathfrak{A}$ is the same as in Theorem 9. As X we take the set s_ω. □

From Theorem 9 it is possible to obtain as a corollary Section 22's theorem on the existence of a model.

THEOREM 22.5. *If a set* Γ *of formulas of a signature* Σ *is consistent, then* Γ *has a model.*

PROOF. By virtue of the compactness theorem it suffices to prove the theorem for a finite set $\Gamma = \{\Phi_1, \ldots, \Phi_k\}$. If Γ is satisfiable and compatible, then so is respectively the sentence $\Psi = \exists x_1 \ldots \exists x_n (\Phi_1 \wedge \ldots \wedge \Phi_k)$, where $x_1, \ldots, x_n$ are all free variables occurring in $\Phi_1, \ldots, \Phi_k$. If $\{\Psi\}$ is compatible, then it follows from Proposition 1 that there is a mechanism of compatibility S for which $\{\Psi\} \in S$. Now we apply Theorem 9 for $s^* = \{\Psi\}$. □

DEFINITION. A set Z of formulas of a signature Σ whose free variables are contained in a set $\{v_1, \ldots, v_n\}$ is an *n-type* of Σ. If T is a consistent theory of Σ, then an n-type Z of Σ is said to be a *principal-in-T n*-type if there is a formula $\Phi(v_1, \ldots, v_n)$ of Σ such that $T \cup \{\exists v_1 \ldots \exists v_n \Phi\}$ is compatible and $T \rhd \Phi \to \Psi$ for any $\Psi \in$ $\in Z$. We shall say that an n-type Z of Σ *is realizable in an algebraic system* $\mathfrak{A}$ of Σ if there are elements $a_1, \ldots, a_n \in A$ such that $\mathfrak{A} \models \Psi(a_1, \ldots, a_n)$ for any formula $\Psi(v_1, \ldots, v_n) \in Z$. If an n-type Z of Σ is not realizable in a system $\mathfrak{A}$ of Σ, then we say that Z is *omitted at* $\mathfrak{A}$.

The following theorem is called the *theorem on the omission of types*.

THEOREM 11. *If* T *is a consistent theory of* Σ *and* Z_i, $i \in \omega$, *are nonprincipal-in-T* n_i*-types of* Σ, *then there is a model* T *of* Σ *omitting all types* Z_i, $i \in \omega$.

PROOF. Consider a collection S of finite sets s of sentences of Σ^c such that $s \cup T$ is compatible. By Proposition 1 S is a mechanism of compatibility. Let f_i, $i \in \omega$, be distinct-valued mappings of ω onto C^{n_i} and let g be a distinct-valued mapping of ω onto ω^2. We define a set X_k, $k \in \omega$, as follows: if $g(k) = \langle i, j\rangle$ and $f_i(j) =$ $= \langle c_1, \ldots, c_{n_i}\rangle$, then we set $X_k = \{\neg(\Phi)^{v_1, \ldots, v_{n_i}}_{c_1, \ldots, c_{n_i}} \mid \Phi \in Z_i\}$. Suppose that the hypothesis of Theorem 10 does not hold. Then there are $s_0 \in S$ and $k_0 \in \omega$ such that $s_0 \cup T \cup \{\Psi\}$ is incompatible for any $\Psi \in X_{k_0}$. Let $g(k_0) = \langle i_0, l\rangle, f_{i_0}(l) = \langle c_1, \ldots, c_{n_{i_0}}\rangle$ and let Φ_0 be the conjunction of all elements s_0. Then $\{\Phi_0\} \cup T$ is compatible and $T \rhd \Phi_0 \to (\Phi)^{v_1, \ldots, v_{n_{i_0}}}_{c_1, \ldots, c_{n_{i_0}}}$ for all $\Phi(v_1, \ldots, v_{n_{i_0}}) \in Z_{i_0}$. Let

$c_{n_{i0}+1}, \dots, c_m$ be all elements of C distinct from $c_1, \dots, c_{n_{i0}}$ and contained in Φ_0. Let Φ_1 be a sentence congruent to the sentence Φ_0 and containing no variables $v_1, \dots, v_m$ and let Φ_2 be a formula of Σ for which $(\Phi_2)^{v_1, \dots, v_m}_{c_1, \dots, c_m} = \Phi_1$. We show that $T \rhd \exists v_{n_{i0}+1} \dots \exists v_m \Phi_2 \to \Phi$ for all $\Phi \in Z_{i0}$. Indeed, let $\mathfrak{A} \models \Phi_2[\gamma]$ for some model $\mathfrak{A}$ of a theory T, having a signature Σ, and some interpretation $\gamma: \{v_1, \dots, v_m\} \to A$. Consider an expansion $\mathfrak{A}'$ of a system $\mathfrak{A}$ to a signature Σ^c such that $\nu^{\mathfrak{A}'}(c_1) = \gamma(v_1), \dots, \nu^{\mathfrak{A}'}(c_m) = \gamma(v_m)$. Then $\mathfrak{A}' \models \Phi_1$ and from the equivalence $\Phi_1 \equiv \Phi_0$ we get $\mathfrak{A}' \models \Phi_0$. Since $\mathfrak{A}'$ is a model of T and $T \rhd \Phi_0 \to (\Phi)^{v_1, \dots, v_{n_{i0}}}_{c_1, \dots, c_{n_{i0}}}$, we have $\mathfrak{A} \models \Phi[\gamma]$. Thus $\mathfrak{A} \models (\exists v_{n_{i0}+1} \dots \exists v_m \Phi_2 \to \Phi)[\gamma]$ for any model $\mathfrak{A}$ of T, any formula $\Phi \in Z_{i0}$ and any interpretation $\gamma: \{v_1, \dots, v_{n_{i0}}\} \to A$. Then it follows from Corollary 22.4 that $T \rhd \exists v_{n_{i0}+1} \dots \exists v_m \Phi_2 \to \Phi$ for any $\Phi \in Z_{i0}$. Since $s_0 \cup T$ is compatible, $T \cup \{\exists v_1 \dots \exists v_m \Phi_2\}$ is also compatible. This contradicts the fact that Z_{i0} is nonprincipal n_{i0}-type. Thus the hypotheses of Theorem 10 hold and hence there is a set X of sentences of Σ^c such that $X \cap X_i \neq \varnothing$, $i \in \omega$, and there is a system $\mathfrak{A}$ of Σ^c which is a model of $T \cup X$ in which any element $a \in A$ is the value of some constant $c \in C$. Since for any $i \in \omega$ and any suite $\langle c_1, \dots, c_{n_i} \rangle \in C^{n_i}$ there is $k \in \omega$ such that $X_k \{\neg(\Phi)^{v_1, \dots, v_{n_i}}_{c_1, \dots, c_{n_i}} \mid \Phi \in Z_i\}$, $\mathfrak{A} \restriction \Sigma$ omits all types Z_i, $i \in \omega$. □

The omission of types theorem is a very important method of constructing models. It supplements the compactness theorem which is mostly used when it is necessary to realize compatible types. Applications of Theorem 11 are given in Sec. 29.

An occurrence of a symbol q in a formula Φ not containing the connective $\to$ is said to be *positive* (*negative*) if the number of different subformulas of Φ of the form $\neg\Psi$ containing that occurrence is even (odd). We denote by $\Sigma^+(\Phi)$ and $\Sigma^-(\Phi)$ sets of relation symbols of Σ having respectively positive and negative occurrences in Φ. For example, if

$$\Phi = \forall v_1(\neg(\exists v_2 r(t_1, v_2) \vee \neg s(v_2)) \wedge \neg(\neg r(v_3, t_2) \wedge v_1 \approx t_1)),$$

where t_1, t_2 are terms, then $\Sigma^+(\Phi) = \{r, s\}$, $\Sigma^-(\Phi) = \{r\}$.

The following theorem is called the *Craig-Lyndon interpolation theorem.*

THEOREM 12. *Let* Φ, Ψ *be sentences of a signature* Σ *not containing the connective* $\to$ *and let* $\Phi \rhd \Psi$. *Then*

(a) *there is a sentence* X *of* Σ *not containing* $\to$ *such that* $\Phi \rhd X$, $X \rhd \Psi$, $\Sigma^+(X) \subseteq \Sigma^+(\Phi) \cap \Sigma^+(\Psi)$ and $\Sigma^-(X) \subseteq \Sigma^-(\Phi) \cap \Sigma^-(\Psi)$;

(b) *if* Σ *contains no function and constant symbols,* Φ *and* Ψ *are without equality and* $\neg\Phi$ *and* Ψ *are both unprovable, then it is possible to require in* (a) *that* X *should be without equality.*

PROOF. A sentence X satisfying the conditions of statement (a) will be called an interpolating sentence for a pair $\langle \Phi, \Psi \rangle$.

(a) Let S be a set of finite sets s of sentences of Σ^c containing no implication symbol which satisfy the following condition: there are $s_1 \neq \varnothing$ and $s_2 \neq \varnothing$ such that $s = s_1 \cup s_2$ and there is no interpolating sentence for the pair $\langle \wedge s_1, \neg(\wedge s_2) \rangle$. (By $\wedge s$ we denote a conjunction of the elements of s.) A set s_1 is called the beginning and s_2 the end of s*. We check conditions (C1) to (C9) of the mechanism of compatibility. Since implication does not occur in the elements of $s \in S$, (C3) trivially holds. If a sentence Θ_1 of Σ^c is equivalent to a sentence $\Theta_2 \in s \in S$ and $\Sigma^\tau(\Theta_1) = \Sigma^\tau(\Theta_2)$, $\tau \in \{+, -\}$; then it is obvious that $s \cup \{\Theta_1\} \in S$. From this we obtain conditions (C2) and (C8). Let $s \in S$. Let s_1 be the beginning of s and s_2 the end of s.

(C1) Let $\{\Theta, \neg\Theta\} \subseteq s$. If $\{\Theta, \neg\Theta\}$ is contained in the beginning (the end) of s, then the sentence $\forall v_1 \neg v_1 \approx v_1$ (the sentence $\forall v_1 v_1 \approx v_1$) will be an interpolating sentence for $\langle \wedge s_1, \neg(\wedge s_2) \rangle$, which contradicts the condition. If $\Theta \in s_1$ and $\neg\Theta \in s_2$ ($\neg\Theta \in s_1$ and $\Theta \in s_2$), then an interpolating sentence for $\langle \wedge s_1, \neg(\wedge s_2) \rangle$ will be a sentence Θ (a sentence $\neg\Theta$).

(C4) Let $\Theta_1 \wedge \Theta_2 \in s_1$ and suppose that there is an interpolating sentence X for $\langle (\wedge s_1) \wedge \Theta_1, \neg(\wedge s_2) \rangle$ or for $\langle (\wedge s_1) \wedge \Theta_2, \neg(\wedge s_2) \rangle$. Then it follows from $\wedge s_1 \rhd \Theta_1$ and $\wedge s_1 \rhd \Theta_2$ that X is an interpolating sentence for $\langle \wedge s_1, \neg(\wedge s_2) \rangle$, which is impossible. If $\Theta_1 \wedge \Theta_2 \in s_2$ and X is an interpolating sentence for $\langle \wedge s_1, \neg((\wedge s_2) \wedge \Theta_1) \rangle$ or for $\langle \wedge s_1, \neg((\wedge s_2) \wedge \Theta_2) \rangle$, then by virtue of $\neg(\wedge s_2 \wedge \Theta_1) \rhd \neg(\wedge s_2)$ and $\neg(\wedge s_2 \wedge \Theta_2) \rhd \neg(\wedge s_2)$ X is an interpolating sentence for $\langle \wedge s_1, \neg(\wedge s_2)\rangle$. The results obtained contradict the condition, which shows that $s \cup \{\Theta_1\} \in S$ and $s \cup \{\Theta_2\} \in S$.

---

* Note that the beginning and the end of s are not determined from s uniquely.

(C5) Let $\Theta_1 \vee \Theta_2 \in s_1$ and X_1, X_2 are interpolating sentences for $\langle(\wedge s_1) \wedge \Theta_1, \neg(\wedge s_2)\rangle$, $\langle(\wedge s_1) \wedge \Theta_2, \neg(\wedge s_2)\rangle$ respectively. Then $X_1 \vee X_2$ will be an interpolating sentence for $\langle \wedge s_1, \neg(\wedge s_2)\rangle$. If $\Theta_1 \vee \Theta_2 \in s_2$ and X_1, X_2 are interpolating sentences for $\langle \wedge s_1, \neg((\wedge s_2) \wedge \Theta_1)\rangle$, $\langle \wedge s_1, \neg((\wedge s_2) \wedge \Theta_2)\rangle$ respectively, then $X_1 \wedge X_2$ is an interpolating sentence for $\langle \wedge s_1, \neg(\wedge s_2)\rangle$.

(C6) Let $\forall x\Theta \in s_2$, $c \in C$ and suppose that X is an interpolating sentence for $\langle \wedge s_1, \neg((\wedge s_2) \wedge (\Theta)^x_c)\rangle$. Since $\neg((\wedge s_2) \wedge (\Theta)^x_c) \rhd \neg(\wedge s_2)$, X is interpolating sentence for $\langle \wedge s_1, \neg(\wedge s_2)\rangle$, which is impossible. For $\forall x\Theta \in s_1$ it similarly follows that $s_1 \cup \{(\Theta)^x_c\}$ may be taken as the beginning and s_2 as the end of $s \cup \{(\Theta)^x_c\}$.

(C7) Suppose $c_0 \in C$ is not contained in the elements of s. If $\exists x\Theta \in s_1$ and **X** is an interpolating sentence for $\langle(\wedge s_1) \wedge (\Theta)^x_c, \neg(\wedge s_2)\rangle$, then it follows from Axiom 12 and Rule 3 of $\mathrm{CP}^{\Sigma^c}_1$ that $\exists y X_1$ is an interpolating sentence for $\langle \wedge s_1, \neg(\wedge s_2)\rangle$, where X_1 contains no constant c_0, $(X_1)^y_{c_0} = X$ and y is a variable not occurring in the elements of $s \cup \{X\}$. In the case where $\exists x\Theta \in s_2$ and X is an interpolating sentence for $\langle \wedge s_1, \neg((\wedge s_2) \wedge (\Theta)^x_{c_0})\rangle$ the sentence $\forall y X_1$ is an interpolating sentence for $\langle \wedge s_1, \neg(\wedge s_2)\rangle$. Indeed, $\wedge s_1 \rhd \forall y X_1$ follows from $\wedge s_1 \rhd X$, since c does not occur in $\wedge s_1$. From $X \rhd \neg((\wedge s_2) \wedge (\Theta)^x_c)$ we get $\forall y X_1 \rhd \neg(\wedge s_2) \vee \forall y \neg(\Theta)^x_y$. If $\forall y X_1 \rhd \neg(\wedge s_2)$ does not hold, then there is a model $\mathfrak{A}$ of the set $\{\forall y X_1, \wedge s_2\}$. It follows from the foregoing that $\forall y \neg(\Theta)^x_y$ is true in $\mathfrak{A}$. This contradicts $\mathfrak{A} \models \wedge s_2$ and $\exists x\Theta \in s_2$.

(C9) Suppose that $c' \in C$ does not occur in the elements of s. If X is an interpolating sentence for $\langle(\wedge s_1) \wedge c' \approx f(c_1, \dots, c_n), \neg(\wedge s_2)\rangle$, then X is an interpolating sentence for $\langle \wedge s_1, \neg(\wedge s_2)\rangle$. Let $\{c_0 \approx f(c_1, \dots, c_n), (\Theta)^x_{f(c_1, \dots, c_n)}\} \subseteq s$. If $\Theta^x_{f(c_1, \dots, c_n)} \in s_1$ and X is an interpolating sentence for $\langle(\wedge s_1) \wedge (\Theta)^x_{c_0}, \neg(\wedge s_2)\rangle$, then an interpolating sentence for $\langle(\wedge s_1), \neg(\wedge s_2)\rangle$ is X in case $c_0 \approx f(c_1, \dots, c_n) \in s_1$ and the sentence $\neg c_0 \approx f(c_1, \dots, c_n) \vee X$ in case $c_0 \approx f(c_1, \dots, c_n) \in s_2$. If $(\Theta)^x_{f(c_1, \dots, c_n)} \in s_2$ and X is an interpolating sentence for $\langle \wedge s_1, \neg((\wedge s_2) \wedge (\Theta)^x_{c_0})\rangle$, then an interpolating sentence for $\langle \wedge s_1, \neg(\wedge s_2)\rangle$ is X in case $c_0 \approx f(c_1, \ldots, c_n) \in s_2$ and the sentence $c_0 \approx f(c_1, \ldots, c_n) \wedge \mathrm{X}$ in case $c_0 \approx f(c_1, \ldots, c_n) \in s_1$.

So we have shown that S is a mechanism of compatibility. If (a) did not hold, the set $\{\Phi, \neg\Psi\}$ would be in S. By Theorem 9 the set $\{\Phi, \neg\Psi\}$ would have a model, which would contradict the condition $\Phi \rhd \Psi$ by virtue of Corollary 22.4.

To prove (b) it is necessary to replace in the definition of S the words "sentence" by "sentence without equality" and require that neither $\rhd \neg(\wedge s_1)$ nor $\rhd \neg(\wedge s_2)$ should hold. Then the cases $\{\Theta, \neg\Theta\} \subseteq s_1$ and $\{\Theta, \neg\Theta\} \subseteq s_2$ are found to be impossible in checking (C1). For the rest checking conditions (C1) to (C7) is the same as in (a). Hence S is a mechanism of compatibility without equality. We then apply Theorem 9′ instead of Theorem 9. ☐

If equality occurs in Φ or in Ψ, then it is impossible to require in Theorem 12(b) that equality should occur in X only when it does in Φ and Ψ (see Exercise 1). In the remainder of this section we apply Theorem 12 to characterize sentences remaining true when passing to homomorphic images.

DEFINITION. If $\mathfrak{A}$ is an algebraic system of Σ, then the relation E on a set A is said to be a *congruence* on $\mathfrak{A}$ if it is an equivalence on A and for any $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$, $r \in R$, $f \in F$, $\mu(r) = \mu(f) = n$, $\langle a_1, b_1\rangle \in E, \ldots, \langle a_n, b_n\rangle \in E$, $\langle a_1, \ldots, a_n\rangle \in \nu^{\mathfrak{A}}(r)$ implies $\langle b_1, \ldots, b_n\rangle \in \nu^{\mathfrak{A}}(r)$ and $\langle a_1, b_1\rangle \in E, \ldots, \langle a_n, b_n\rangle \in E$ implies $\langle \nu^{\mathfrak{A}}(f)(a_1, \ldots, a_n), \nu^{\mathfrak{A}}(f)(b_1, \ldots, b_n)\rangle \in E$. If E is a congruence on the system $\mathfrak{A}$ of Σ, then we define a new system $\mathfrak{A}/E$ of Σ which we call a *factor system of the system* $\mathfrak{A}$ *with respect to E.* The carrier $\mathfrak{A}/E$ consists of equivalence classes $aE = \{b \mid \langle b, a\rangle \in E\}$. The interpretation $\nu^{\mathfrak{A}/E}$ is defined as follows:

$$\langle a_1E, \ldots, a_nE\rangle \in \nu^{\mathfrak{A}/E}(r) \Leftrightarrow \langle a_1, \ldots, a_n\rangle \in \nu^{\mathfrak{A}}(r) \quad (r \in R)$$

$$\nu^{\mathfrak{A}/E}(f)(a_1E, \ldots, a_nE) = \nu^{\mathfrak{A}}(f)(a_1, \ldots, a_n)E \quad (f \in F).$$

Verification of the correctness of this definition, as well as the proof of the following simple proposition, will be left as an exercise to the reader.

PROPOSITION 3. (a) *Let* Φ *be a sentence of* Σ *and let* Φ' *be obtained from* Φ *by replacing subformulas* $t_1 \approx t_2$ *by* $E(t_1, t_2)$, *where*

E is a relation symbol not occurring in R. If $\mathfrak{A}$ is a system of $\Sigma' \supseteq \Sigma$, $E \in R'$ and $\nu^{\mathfrak{A}}(E)$ is a congruence on $\mathfrak{A} \upharpoonright \Sigma$, then

$$\mathfrak{A} \models \Phi' \Leftrightarrow \mathfrak{A}/\nu^{\mathfrak{A}}(E) \models \Phi.$$

(b) *If E is a congruence on a system $\mathfrak{A}$, then the mapping assigning to an element $a \in A$ an element aE is a homomorphism of $\mathfrak{A}$ onto $\mathfrak{A}/$E.* □

A formula Φ is said to be *positive* if it contains no implication and all the occurrences in Φ of relation and equality symbols are positive. We shall say that a sentence Φ of Σ is preserved *under homomorphisms with respect to a sentence* Ψ of Σ if the truth of $\Phi \wedge \Psi$ on a system $\mathfrak{A}$ of Σ implies the truth of $\Phi \wedge \Psi$ on any of its homomorphic images.

THEOREM 13. *Let Φ and Ψ be sentences of Σ and let the sentence $\Psi \to \neg\Phi$ be unprovable. For Φ to be preserved under homomorphisms with respect to Ψ it is necessary and sufficient that Φ be equivalent to a positive sentence* X *with respect to Ψ* (i. e. $\Psi \rhd (\Phi \to \mathrm{X}) \wedge (\mathrm{X} \to \Phi)$).

PROOF. Necessity. Since Φ and Ψ contain a finite number of symbols, the signature $\Sigma = \langle R, F, \mu\rangle$ may be assumed finite. Suppose first $F = \varnothing$. Denote by Θ a conjunction of sentences

$$\forall v_1 \ldots \forall v_n(\neg r(v_1, \ldots, v_n) \vee r'(v_1, \ldots, v_n)), \quad r \in R, \quad \mu(r) = n,$$

and a sentence

$$\forall v_1 \forall v_2(\neg E(v_1, v_2) \vee E'(v_1, v_2)),$$

where $r'(r \in R)$, E and E' are pairwise distinct symbols not in R. Denote by Δ a signature sentence containing only symbols of $R \cup \{E\}$ and no implication symbol whose truth on a system $\mathfrak{A}$ is equivalent to the fact that $\nu^{\mathfrak{A}}(E)$ is a congruence on $\mathfrak{A} \upharpoonright \Sigma$. Let Φ_0 and Ψ_0 be obtained from Φ and Ψ respectively by replacing all formulas of the form $x \approx y$ by $E(x, y)$. Let Φ_0', Ψ_0' and Δ' be obtained from Φ_0, Ψ_0 and Δ respectively by replacing all predicate symbols by primed symbols. If a sentence $\Theta \wedge \Delta \wedge \Delta'$ is true on $\mathfrak{A}$, then $\nu^{\mathfrak{A}}(r) \subseteq \nu^{\mathfrak{A}}(r')$ for $r \in R$ and $\nu^{\mathfrak{A}}(E) \subseteq \nu^{\mathfrak{A}}(E')$ and so the mapping assigning to an element aE an element aE' is a homomorphism of $(\mathfrak{A} \upharpoonright \Sigma)/\nu^{\mathfrak{A}}(E)$ onto $\mathfrak{A}_1/\nu^{\mathfrak{A}'}(E')$ where $\mathfrak{A}_1 = \langle A, \nu^{\mathfrak{A}_1}\rangle$ is a system of Σ for which $\nu^{\mathfrak{A}_1}(r) = \nu^{\mathfrak{A}}(r')(r \in R)$.

From this, via Corollary 22.4, Proposition 3(a) and the hypothesis of the theorem we get

$$\Psi_0 \wedge \Phi_0 \wedge \Delta \rhd \neg \Psi_0' \vee \neg \Theta \vee \neg \Delta' \vee \Phi_0'.$$

Suppose that $\rhd \neg \Psi_0' \vee \neg \Theta \vee \neg \Delta' \vee \Phi_0'$. On replacing in the proof the symbols r' by r for $r \in R$ and E' by E we get

$$\rhd \neg \Psi_0 \vee \neg \Theta_1 \vee \neg \Delta \vee \Phi_0,$$

where Θ_1 is obtained from Θ by replacing r' by r for $r \in R$ and E' by E. It is clear that $\rhd \Theta_1$ and hence $\neg \Psi_0 \vee \neg \Delta \vee \Phi_0$ is an identically true sentence. From this, using the fact that Δ is true on systems $\mathfrak{A}$ in which the relation $\nu^{\mathfrak{A}}(E)$ is an equality, we conclude that $\Psi \to \Phi$ is also identically true. We may take as X therefore a sentence $\forall v_1\, v_1 \approx v_1$. Now let $\neg \Psi_0' \vee \neg \Theta \vee \neg \Delta' \vee \Phi_0'$ be unprovable. The sentence $\neg(\Psi_0 \wedge \Phi_0 \wedge \Delta)$ is also unprovable, since otherwise by virtue of the fact that Δ is true on systems $\mathfrak{A}$ in which $\nu^{\mathfrak{A}}(E)$ is an equality, the sentence $\Psi \to \neg \Phi$ would also be identically true, which contradicts the condition that it is unprovable. Then by Theorem 12(b) there is an interpolating sentence X_0 containing no equality for which the following conditions hold: $\Psi_0 \wedge \Phi_0 \wedge \Delta \rhd \mathrm{X}_0$, $\mathrm{X}_0 \rhd \neg \Psi_0' \vee \neg \Theta \vee \neg \Delta' \vee \Phi_0'$, $\Sigma^+(\mathrm{X}_0) \subseteq R \cup \{E\}$ and $\Sigma^-(\mathrm{X}_0) \subseteq \Sigma^-(\Psi_0 \wedge \Phi_0 \wedge \Delta) \cap \Sigma^-(\neg \Psi_0' \vee \neg \Theta \vee \neg \Delta' \vee \Phi_0') = \varnothing$. Hence X_0 is a positive sentence of a signature Σ_1 which contains only the symbol E in addition to those of Σ. Replacing in the derivation the symbols r' by r for $r \in R$ and E' by E yields $\mathrm{X}_0 \rhd \neg \Psi_0 \vee \neg \Theta_1 \vee \neg \Delta \vee \Phi_0$. Since $\rhd \Theta_1$, we have $\mathrm{X}_0 \rhd \neg \Psi_0 \vee \neg \Delta \vee \Phi_0$. We have thus obtained $\Psi_0, \Delta \rhd (\Phi_0 \to \mathrm{X}_0) \wedge (\mathrm{X}_0 \to \Phi_0)$. Since Δ is true on systems $\mathfrak{A}$ in which the relation $\nu^{\mathfrak{A}}(E)$ is an equality, $\Psi \rhd (\Phi \to \mathrm{X}) \wedge (\mathrm{X} \to \Phi)$ for the positive sentence X obtained from X_0 by replacing subformulas of the form $E(x, y)$ by $x \approx y$.

Now let $\Sigma = \langle R, \{f_1, \ldots, f_m\}, \mu\rangle$. Consider a signature $\Sigma' = \langle R \cup \{F_1, \ldots, F_m\}, \varnothing, \mu'\rangle$, where $F_1, \ldots, F_m$ are pairwise distinct symbols not in R, $\mu'(r) = \mu(r)$ $(r \in R)$ and $\mu'(F_i) = \mu(f_i) + 1$, $i \in \{1, \ldots, m\}$. Let Ψ_0 be a sentence expressing in the systems of Σ' that the relations $F_1, \ldots, F_m$ are functions *. Let Φ_1,

---

* That is, Ψ_0 is a conjunction of the sentences $\forall x_1 \ldots \forall x_{n_i} \forall y \forall z ((F_i(x_1, \ldots, x_{n_i}, y) \wedge F_i(x_1, \ldots, x_{n_i}, z)) \to y \approx z) \wedge \forall x_1 \ldots \forall x_{n_i} \exists y F_i(x_1, \ldots, x_{n_i}, y)$, $i \in \{1, \ldots, m\}$, $n_i = \mu(f_i)$.

Ψ_1 be sentences of Σ_1 in reduced nf equivalent to the sentences Φ and Ψ respectively. Let Φ_2, Ψ_2 be obtained from Φ_1, Ψ_1 respectively by replacing atomical subformulas of the form $y \approx f_i(x_1, \dots, x_n)$, $f_i(x_1, \dots, x_n) \approx y$ by $F_i(x_1, \dots, x_n, y)$. Clearly if Φ is preserved under homomorphisms with respect to Ψ, then Φ_2 is preserved under homomorphisms with respect to $\Psi_0 \wedge \Psi_2$. Since Σ' contains no function symbols, it follows from the foregoing that there is a sentence X_1 of Σ' for which

$$\Psi_0 \wedge \Psi_2 \rhd (\Phi_2 \rightarrow \mathrm{X}_1) \wedge (\mathrm{X}_1 \rightarrow \Phi_2).$$

Using Corollary 22.4 we then get

$$\Psi \rhd (\Phi \rightarrow \mathrm{X}) \wedge (\mathrm{X} \rightarrow \Phi),$$

where X is a positive sentence of Σ obtained from X_1 by replacing $F_i(x_1, \dots, x_{n+1})$ by $x_{n+1} \approx f(x_1, \dots, x_n)$.

The sufficiency of the hypothesis of the theorem is obtained from the following two facts which are verified directly by induction on the length of X. (a) If h is a homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$ and $\mathrm{X}(x_1, \dots, x_n)$ is a formula containing no negation, then

$$\mathfrak{A} \models \mathrm{X}(a_1, \dots, a_n) \Rightarrow \mathfrak{B} \models \mathrm{X}(ha_1, \dots, ha_n).$$

(b) A positive formula X is equivalent to formula X_1 containing no negation. □

COROLLARY 1. If K is an axiomatizable class, then K is closed under Homomorphic images if and only if K has a system of axioms consisting of positive sentences. □

Exercises

1. Using Theorem 11 prove that for any countable linear ordering $\mathfrak{B}$ without the last element there is a proper elementary extension of $\mathfrak{B}$ (i. e. $\mathfrak{A} \prec \mathfrak{B}$ and $A \neq B$) such that $\mathfrak{A}$ is the initial segment of $\mathfrak{B}$ (i. e. it follows from $\langle b, a \rangle \in \nu^{\mathfrak{B}}(\leqslant)$ and $a \in A$ that $b \in A$). (*Hint.* Add to the signature the constants $\{c\} \cup \{c_a \mid a \in A\}$, consider a theory T with a set of axioms $D^*(\mathfrak{A}) \cup \{\neg c \approx c_a \mid a \in A\}$ and the types $Z_b = \{v_1 \leqslant c_b\} \cup \{\neg v_1 \approx c_a \mid a \in A\}$ and use the theorem on the omission of types.)

2. Show that if an equality occurs in Φ or in Ψ, then one cannot require in Theorem 12(b) that an equality should occur in X only when it occurs in Φ and Ψ. (*Hint.* Consider the examples $c_1 \approx c_2 \rhd r(c_1) \vee \neg r(c_2)$, $r(c_1) \wedge \neg r(c_2) \rhd \neg c_1 \approx c_2$.)

3. A formula Ψ is said to be negative if in the formula Ψ_1 obtained from Ψ by replacing all its subformulas of the form $\Psi_1 \to \Psi_2$ by $\neg\Psi_1 \vee \Psi_2$ each occurrence of a relation symbol and of the equality is negative. Show that provable formulas cannot be negative. (*Hint.* A negative formula is false in E_Σ.)

4. Deduce from Exercise 3 that in Theorem 13 the condition that $\Psi \to \neg\Phi$ is unprovable cannot be omitted.

28. COUNTABLE HOMOGENEITY AND UNIVERSALITY

Let T be a theory of a signature Σ. We denote by $F_n(\Sigma)$ a set of formulas of Σ with free variables of a set $\{v_1, \ldots, v_n\}$. If $\Phi \in$ $\in F_n(\Sigma)$, then by $\|\Phi\|_T$ or simply by $\|\Phi\|$ we denote a set $\{\Psi \in$ $\in F_n(\Sigma) \mid T \rhd (\Phi \to \Psi) \wedge (\Psi \to \Phi)\}$. We denote by $\mathfrak{B}_n(T)$ a Boolean algebra with a carrier $B_n(T) = \{\|\Psi\| \mid \Psi \in F_n(\Sigma)\}$ and the following operations:

(a) $\|\Phi\| \cup \|\Psi\| = \|\Phi \vee \Psi\|$;
(b) $\|\Phi\| \cap \|\Psi\| = \|\Phi \wedge \Psi\|$;
(c) $\overline{\|\Phi\|} = \|\neg\Phi\|$.

Checking the correctness of the definition of the operations, as well as verification of axioms (1) to (10) of Boolean algebras will be left as an exercise to the reader.

Let us suppose that in this section all algebraic systems and theories to be considered have a signature Σ, unless otherwise stated, and that the power of Σ is finite or countable. By a model of a theory T we shall mean a model T of a signature Σ. Let $\mathfrak{A}$ be an algebraic system of Σ and $a_1, \ldots, a_n \in A$. The *type of the collection* $\langle a_1, \ldots, a_n\rangle$ in $\mathfrak{A}$ is the following n-type:

$$T(\mathfrak{A}, a_1, \ldots, a_n) = \\ = \{\Phi(v_1, \ldots, v_n) \mid \mathfrak{A} \models \Phi(a_1, \ldots, a_n),\ \Phi \in F_n(\Sigma)\}.$$

If $\mathfrak{A}, \mathfrak{B}$ are systems of Σ, $a_1, \ldots, a_n \in A$, $b_1, \ldots, b_n \in B$, then the equation $T(\mathfrak{A}, a_1, \ldots, a_n) = T(\mathfrak{B}, b_1, \ldots, b_n)$ will also be denoted by

$$\langle \mathfrak{A}, a_1, \ldots, a_n\rangle \equiv \langle \mathfrak{B}, b_1, \ldots, b_n\rangle.$$

DEFINITION. A countable algebraic system $\mathfrak{A}$ is said to be *homogeneous* if for any $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$ and any element

$a \in A$

$$\langle \mathfrak{A}, a_1, \ldots, a_n \rangle \equiv \langle \mathfrak{A}, b_1, \ldots, b_n \rangle \tag{1}$$

implies

$$\langle \mathfrak{A}, a_1, \ldots, a_n, a \rangle \equiv \langle \mathfrak{A}, b_1, \ldots, b_n, b \rangle \tag{2}$$

for some $b \in A$.

It is clear that if $\mathfrak{A}$ is a homogeneous system and $X \subseteq A$ is a finite set, then the system $\mathfrak{A}_X$ is also homogeneous.

PROPOSITION 1. *For any countable system $\mathfrak{A}$ there is a countable elementary homogeneous extension $\mathfrak{B} > \mathfrak{A}$.*

PROOF. We first show that for any countable system there is a countable elementary extension $\mathfrak{A}^{(1)} > \mathfrak{A}$ such that for any $a_1, \ldots, a_n, b_1, \ldots, b_n, a \in A$ (1) implies

$$\langle \mathfrak{A}^{(1)}, a_1, \ldots, a_n, a \rangle \equiv \langle \mathfrak{A}^{(1)}, b_1, \ldots, b_n, b \rangle \tag{3}$$

for some $b \in A^{(1)}$. For every $X = \{a_1, \ldots, a_n\} \subseteq A$ we define a set

$$R(X) = \{\gamma : X \to A \mid \langle \mathfrak{A}, a_1, \ldots, a_n \rangle \equiv \langle \mathfrak{A}, \gamma a_1, \ldots, \gamma a_n \rangle\}.$$

We denote by F the union of all $R(X)$, where X is a finite subset of A. It is clear that R has a countable power. We extend the signature Σ_A to Σ_1 by adding new symbols of one-place operations f_γ for each $\gamma \in R$. Consider the following set of sentences of Σ_1:

$$Z = D^*(\mathfrak{A}) \cup \{\forall x(\Phi(x, c_{a_1}, \ldots, c_{a_n}) \to \\ \to \Phi(f_\gamma(x), c_{\gamma a_1}, \ldots, c_{\gamma a_n})) \\ \mid \gamma \in R, a_1, \ldots, a_n \in \operatorname{dom} \gamma, \Phi(x, y_1, \ldots, y_n) \in F(\Sigma)\}.$$

It follows from the definition of the set F that every finite set $Z_1 \subseteq Z$ holds in some expansion of $\mathfrak{A}$. Let $\mathfrak{A}_1$ be a countable model of Z and let $\mathfrak{A}^{(1)} = \mathfrak{A}_1 \restriction \Sigma$. Since $\mathfrak{A}$ is a model of $D^*(\mathfrak{A})$, it may be assumed by Proposition 24.4(a) that $\mathfrak{A} < \mathfrak{A}^{(1)}$. If (1) holds, then the truth on $\mathfrak{A}_1$ of the sentences of Z implies that (3) holds for $b = f_\gamma^{\mathfrak{A}_1}(a)$, where $\gamma(a_1) = b_1, \ldots, \gamma(a_n) = b_n$.

We define a sequence of systems $\{\mathfrak{A}_i \mid i \in \omega\}$ as follows: $\mathfrak{A}_0 = \mathfrak{A}$, $\mathfrak{A}_{i+1} = \mathfrak{A}_i^{(1)}$, $i \in \omega$. By Proposition 24.3 we get $\mathfrak{A}_k < \mathfrak{B} = \bigcup_{i \in \omega} \mathfrak{A}_i$, $k \in \omega$ and, in particular, $\mathfrak{A} < \mathfrak{B}$. Since $\mathfrak{B} = \bigcup \mathfrak{A}_i$, we see that $\mathfrak{B}$ is a countable system. If $a_1, \ldots, a_n, b_1, \ldots, b_n, a \in B$ and

$$\langle \mathfrak{B}, a_1, \ldots, a_n \rangle \equiv \langle \mathfrak{B}, b_1, \ldots, b_n \rangle,$$

then $a_1, \ldots, a_n, b_1, \ldots, b_n, a \in A_i$ for some $i \in \omega$. Since $\mathfrak{A}_i < \mathfrak{B}$ we have

$$\langle \mathfrak{A}_i, a_1, \ldots, a_n \rangle \equiv \langle \mathfrak{A}_i, b_1, \ldots, b_n \rangle.$$

From the definition of $\mathfrak{A}_i^{(1)} = \mathfrak{A}_{i+1}$ we get

$$\langle \mathfrak{A}_{i+1}, a_1, \ldots, a_n, a \rangle \equiv \langle \mathfrak{A}_{i+1}, b_1, \ldots, b_n, b \rangle$$

for some $b \in A_{i+1}$. Since $\mathfrak{A}_{i+1} < \mathfrak{B}$, we have

$$\langle \mathfrak{B}, a_1, \ldots, a_n, a \rangle \equiv \langle \mathfrak{B}, b_1, \ldots, b_n, b \rangle.$$

Thus $\mathfrak{B} > \mathfrak{A}$ is a countable homogeneous system. □

PROPOSITION 2. *Let $\mathfrak{A}, \mathfrak{B}$ be countable homogeneous systems of a signature Σ. Then the following conditions are equivalent*:

(a) $\mathfrak{A} \simeq \mathfrak{B}$,

(b) *the same n-types of Σ, $n \in \omega$, are realized in $\mathfrak{A}$ and $\mathfrak{B}$.*

PROOF. (a) $\Rightarrow$ (b) is obvious. Let (b) hold. We number A and B: $A = \{a_i \mid i \in \omega\}$, $B = \{b_i \mid i \in \omega\}$. By induction on $n \in \omega$ we construct finite mappings $f_n \colon A_n \to B$, $A_n \subseteq A$, with the following properties:

(1_n) if $n \neq 0$, then $f_{n-1} \subseteq f_n$;

(2_n) if $n = 2k + 1$, then $a_k \in A_n$;

(3_n) if $n = 2(k + 1)$, then $b_k \in f_n(A_n)$;

(4_n) if $A_n = \{e_1, \ldots, e_m\}$, then

$$\langle \mathfrak{A}, e_1, \ldots, e_m \rangle \equiv \langle \mathfrak{B}, f_n e_1, \ldots, f_n e_m \rangle.$$

For $f_0 = \varnothing$ conditions (1_0) to (3_0) trivially hold. Condition (4_0) follows from (b), since $\mathrm{Th}(\mathfrak{A})$ is a 0-type. Let $n = 2k + 1$ and $A_{n-1} = \{e_1, \ldots, e_m\}$. By the induction hypothesis

$$\langle \mathfrak{A}, e_1, \ldots, e_m \rangle \equiv \langle \mathfrak{B}, f_{n-1} e_1, \ldots, f_{n-1} e_m \rangle. \tag{1}$$

It follows from condition (b) that the type $T(\mathfrak{A}, e_1, \ldots, e_m, a_k)$ is realizable in $\mathfrak{B}$ and therefore

$$\langle \mathfrak{A}, e_1, \ldots, e_m, a_k \rangle \equiv \langle \mathfrak{B}, d_1, \ldots, d_{m+1} \rangle \tag{2}$$

for some $d_1, \ldots, d_{m+1} \in B$. From (1) and (2) we get

$$\langle \mathfrak{B}, d_1, \ldots, d_m \rangle \equiv \langle \mathfrak{B}, f_{n-1} e_1, \ldots, f_{n-1} e_m \rangle;$$

therefore by virtue of the homogeneity of $\mathfrak{B}$ there is $b \in B$ such that

$$\langle \mathfrak{B}, d_1, \ldots, d_{m+1} \rangle \equiv \langle \mathfrak{B}, f_{n-1}e_1, \ldots, f_{n-1}e_m, b \rangle.$$

By virtue of (2) we then have

$$\langle \mathfrak{A}, e_1, \ldots, e_m, a_k \rangle \equiv \langle \mathfrak{B}, f_{n-1}e_1, \ldots, f_{n-1}e_m, b \rangle$$

and consequently the mapping $f_n = f_{n-1} \cup \{\langle a_k, b \rangle\}$ will satisfy conditions (1_n) to (4_n). The case $n = 2(k+1)$ is treated similarly. It follows from conditions (1_n) to (4_n), $n \in \omega$, that $f = \bigcup_{n \in \omega} f_n$ will be an isomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$. □

DEFINITION. A countable algebraic system $\mathfrak{A}$ of Σ is said to be *universal* if for any $n \in \omega$ all n-types of Σ compatible with $\mathrm{Th}(\mathfrak{A})$ are realized in it. A countable algebraic system $\mathfrak{A}$ of Σ is said to be *saturated* if for any finite $X \subseteq A$ all 1-types of Σ_X compatible with $\mathrm{Th}(\mathfrak{A}_X)$ are realized in $\mathfrak{A}_X$.

It is clear that the compatibility of the n-type of Z with $\mathrm{Th}(\mathfrak{A})$ is equivalent to the local satisfiability of Z in $\mathfrak{A}$. It is obvious that a countable elementary extension of a universal system is a universal system. It is also clear that if a system $\mathfrak{A}$ is saturated, then the system $\mathfrak{A}_X$ is also saturated for any finite $X \subseteq A$.

PROPOSITION 3. *For a countable algebraic system* $\mathfrak{A}$ *the following conditions are equivalent*:

(1) $\mathfrak{A}$ *is saturated*,

(2) $\mathfrak{A}$ *is universal and homogeneous.*

PROOF. (1) ⇒ (2). Let $\mathfrak{A}$ be saturated. We show by induction on $n \in \omega$ that any n-type Z_0 of Σ compatible with $\mathrm{Th}(\mathfrak{A})$ is satisfiable in $\mathfrak{A}$. If $n = 1$, the satisfiability of Z_0 in $\mathfrak{A}$ follows from the definition of saturation. Let $n > 1$. Consider the $(n-1)$-type $Z_1 = \{\exists v_n(\Phi_1 \wedge \ldots \wedge \Phi_k) \mid \Phi_1, \ldots, \Phi_k \in Z_0\}$. Since Z_1 is locally satisfiable in $\mathfrak{A}$, by the induction hypothesis the type Z_1 is realized in $\mathfrak{A}$ by the elements $a_1, \ldots, a_{n-1}$. It will be assumed that v_1 does not occur bound in the elements of Z_0. By virtue of Proposition 19.4(b) it suffices to consider only such n-types Z_0. Consider the 1-type

$$Z_2 = \left\{(\Phi)^{v_1, \ldots, v_{n-1}, v_n}_{c_{a_1}, \ldots, c_{a_{n-1}}, v_1} \middle| \Phi \in Z_0\right\}.$$

It is clear that the 1-type Z_2 is locally satisfiable in $\mathfrak{A}_{\{a_1, \dots, a_{n-1}\}}$. By the saturation of $\mathfrak{A}$ there is an element $a \in A$ realizing in $\mathfrak{A}_{\{a_1, \dots, a_{n-1}\}}$ the type Z_2. Hence the n-type Z_0 is realized in $\mathfrak{A}$ by the elements $a_1, \dots, a_{n-1}, a$.

We show that $\mathfrak{A}$ is homogeneous. Let $a_1, \dots, a_n, b_1, \dots, b_n, a \in A$ and

$$\langle \mathfrak{A}, a_1, \dots, a_n \rangle \equiv \langle \mathfrak{A}, b_1, \dots, b_n \rangle. \tag{$*$}$$

Consider a 1-type

$$Z_0 = \{\Phi(v_1) \mid \mathfrak{A}_{\{a_1, \dots, a_n\}} \vDash \Phi(a), \Phi \in F_1(\Sigma_{\{a_1, \dots, a_n\}})\}.$$

It follows from ($*$) that a 1-type

$$Z_1 = \left\{(\Phi_1)^{x_1, \dots, x_n}_{c_{b_1}, \dots, c_{b_n}} \middle| (\Phi_1)^{x_1, \dots, x_n}_{c_{a_1}, \dots, c_{a_n}} \in Z_0, \Phi_1(x_1, \dots, x_n, v_1) \in F(\Sigma)\right\}$$

is locally satisfiable in $\mathfrak{A}_{\{b_1, \dots, b_n\}}$. Since $\mathfrak{A}$ is saturated, Z_1 is realized in $\mathfrak{A}_{\{b_1, \dots, b_n\}}$ by an element $b \in A$. It is clear that we then have

$$\langle \mathfrak{A}, a_1, \dots, a_n, a \rangle \equiv \langle \mathfrak{A}, b_1, \dots, b_n, n \rangle.$$

(2) ⇒ (1). Let $\mathfrak{A}$ be universal and homogeneous, $a_1, \dots, a_n \in A$ and Z_0 be a 1-type of $\mathfrak{A}_{\{a_1, \dots, a_n\}}$ locally satisfiable in $\Sigma_{\{a_1, \dots, a_n\}}$. It may be assumed without loss of generality that all bound variables in the elements of Z_0 are different from $v_1, \dots, v_{n+1}$. Consider an n-type $Z_1 = T(\mathfrak{A}, a_1, \dots, a_n)$ and an $(n+1)$-type

$$Z_2 = Z_1 \cup \left\{\Phi \mid (\Phi)^{v_1, \dots, v_n, v_{n+1}}_{c_{a_1}, \dots, c_{a_n}, v_1} \in Z_0, \Phi(v_1, \dots, v_{n+1}) \in F(\Sigma)\right\}.$$

If Z_0 is locally satisfiable in $\mathfrak{A}_{\{a_1, \dots, a_n\}}$, then Z_2 is locally satisfiable in $\mathfrak{A}$. Since $\mathfrak{A}$ is universal, Z_2 is satisfiable in $\mathfrak{A}$ by some $b_1, \dots, b_{n+1} \in A$. Since $Z_1 \subsetneq Z_2$, we have

$$\langle \mathfrak{A}, a_1, \dots, a_n \rangle \equiv \langle \mathfrak{A}, b_1, \dots, b_n \rangle.$$

From the homogeneity of $\mathfrak{A}$ we get

$$\langle \mathfrak{A}, a_1, \dots, a_n, a \rangle \equiv \langle \mathfrak{A}, b_1, \dots, b_{n+1} \rangle$$

for some $a \in A$. It is obvious that a realizes Z_0 in $\mathfrak{A}_{\{a_1, \dots, a_n\}}$. □

PROPOSITION 4. *If* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are countable saturated elementarily equivalent systems, then* $\mathfrak{A} \simeq \mathfrak{B}$.

PROOF. Immediate from Propositions 3 and 2, since all n-types compatible with $\mathrm{Th}(\mathfrak{A}) = \mathrm{Th}(\mathfrak{B})$ are realized in $\mathfrak{A}$ and $\mathfrak{B}$. □

Thus there is a one-to-one correspondence to within isomorphism between complete theories T with countable saturated models and countable saturated models of T. By Proposition 1 any theory T has a countable homogeneous model. Not all theories T, however, have a countable saturated model (see Exercise 2). The following proposition characterizes complete theories T possessing saturated models.

PROPOSITION 5. *For a complete theory* T *possessing infinite models the following conditions are equivalent*:

(1) T *has a countable universal model*;

(2) T *has a countable saturated model*;

(3) *for any* $n \in \omega$ *a Boolean algebra* $\mathfrak{B}_n(T)$ *has a countable number of ultrafilters.*

PROOF. (1) ⇒ (2). Let $\mathfrak{A}$ be a countable universal model of T. By Proposition 1 there is a countable homogeneous model $\mathfrak{B} > \mathfrak{A}$. It follows from Proposition 3 that $\mathfrak{B}$ is a saturated model of T.

(2) ⇒ (3). Suppose $\mathfrak{A}$ is a countable saturated model of T, $n \in$ $\in \omega$ and U is an ultrafilter of an algebra $\mathfrak{B}_n(t)$. Consider an n-type

$$T(U) = \{\Phi \mid \|\Phi\| \in U, \Phi \in F_n(\Sigma)\}.$$

It is clear that $T(U)$ is an n-type compatible with T. Since $\mathfrak{A}$ is universal, there is a collection $\bar{a}(U) = \langle a_1, \ldots, a_n \rangle$ realizing the type $T(U)$ in $\mathfrak{A}$. If U_1, U_2 are two distinct ultrafilters of $\mathfrak{B}_n(T)$, then for some $\Phi \in F_n(\Sigma)$ we have $\|\Phi\| \in U_1$ and $\|\neg\Phi\| \in U_2$. Hence $\bar{a}(U_1) \neq \bar{a}(U_2)$. Thus there is a distinct-valued mapping of the set of all ultrafilters of an algebra $\mathfrak{B}_n(T)$ into a countable set A^n. This yields condition (3).

(3) ⇒ (1). Let $\{U_i^n \mid i \in \omega\}$ be the set of all ultrafilters of $\mathfrak{B}_n(T)$ and suppose that a signature Σ_1 is obtained from Σ by adding to it new pairwise distinct constants $\{c_j^{n,i} \mid n, i \in \omega, 1 \leqslant j \leqslant n\}$. Then a countable set of sentences of Σ

$$X = T \cup \left\{(\Phi)^{v_1, \ldots, v_n}_{c_1^{n,i}, \ldots, c_n^{n,i}} \middle| n, i \in \omega; \Phi \in T(U_i^n)\right\}$$

is compatible. Let $\mathfrak{A}$ be a countable model of X. Then $\mathfrak{A} \upharpoonright \Sigma$ is a universal model of T. Indeed, let Z_0 be an n-type of Σ compatible with T. Then a set $Y = \{ \|\Phi\| \mid \Phi \in Z_0 \}$ is a family of sets with the finite intersection property of $\mathfrak{B}_n(T)$. By Proposition 12.1 there is an ultrafilter $U_i^n \supseteq Y$ of $\mathfrak{B}_n(T)$. Since $Z_0 \subseteq T(U_i^n)$, Z_0 is realized in $\mathfrak{A} \upharpoonright \Sigma$ by the elements $\nu^{\mathfrak{A}}(c_1^{n,i}), \ldots, \nu^{\mathfrak{A}}(c_n^{n,i})$. □

The concepts of a homogeneous, a universal and a saturated countable system easily carry over to other powers. In particular, an algebraic system $\mathfrak{A}$ of Σ is said to be *$\varkappa$-saturated*, where $\varkappa$ is a cardinal, if for any set $X \subseteq A$ of power $< \varkappa$ any 1-type of Σ_X compatible with $\mathrm{Th}(\mathfrak{A}_X)$ is realized in $\mathfrak{A}_X$. To conclude this section, consider a theorem independently proved by Yu. L. Ershov and H. J. Keisler.

A filter D on a set I is said to be *countably complete* if for any set $\{X_i \mid i \in \omega\} \subseteq D$ we have $\bigcap_{i \in \omega} X_i \in D$. We denote by ω_1 the first uncountable cardinal.

PROPOSITION 6. *If $\mathfrak{A}_i$, $i \in I$, are algebraic systems of Σ and D is an ultrafilter on I not countably complete, then the system D-*prod *$\mathfrak{A}_i$ is ω_1-saturated.*

PROOF. Let $\{X_i \mid i \in \omega\} \subseteq D$ and $\bigcap_{i \in \omega} X_i \notin D$. Consider a family $\{W_i \mid i \in \omega\}$, where $W_0 = I \setminus \bigcup_{i \in \omega} X_i$, $W_1 = \bigcap_{i \in \omega} X_i$ and $W_i = (X_0 \cap \ldots \cap X_{i-2}) \setminus (X_0 \cap \ldots \cap X_{i-1})$ for $i \geqslant 2$. It is clear that $W_i \notin D$ for $i \in \omega$, $\bigcup_{i \in \omega} W_i = I$ and $W_i \cap W_j = \varnothing$ for $i \neq j$. Let $\mathfrak{A}_i$, $i \in I$ be algebraic systems of Σ, let $X \subseteq D$-prod A_i, $|X| \leqslant \omega$ and suppose that $Z = \{\Phi_i(v_1) \mid i \in \omega\}$ is a 1-type of Σ_X compatible with $\mathrm{Th}((D\text{-prod } \mathfrak{A}_i)_X)$ and Φ_0 is an identically true formula.

Let $\mathfrak{B} = (D\text{-prod } \mathfrak{A}_i)_X$ and $X = \{Df^k \mid k \in \omega\}$. Consider expansions $\mathfrak{B}_i$ of systems $\mathfrak{A}_i$ of Σ_X for which $c_{Df^k}^{\mathfrak{B}_i} = f^k(i)$. Clearly $\mathfrak{B} = D$-prod $\mathfrak{B}_i$ and for all $k \in \omega$

$$\{i \in I \mid \mathfrak{B}_i \models \exists v_1 (\Phi_0 \wedge \ldots \wedge \Phi_k)\} \in D. \tag{1}$$

We choose $f \in I$-prod B_i so that for any k, $n \in \omega$, $k \in W_n$ there is $\mathfrak{B}_k \models \Phi_0(fk) \wedge \ldots \wedge \Phi_{m(k)}(fk)$, where $m(k)$ is the greatest number in the set $\{0, 1, \ldots, n\}$ for which $\mathfrak{B}_k \models \exists v_1 (\Phi_0 \wedge \ldots \wedge \Phi_{m(k)})$. Since

$W_i \cap W_j = \varnothing$ for $i \neq j$ and Φ_0 is identically true, we can choose such f.

We show that for any $k_0 \in \omega$, $k_0 \geqslant 1$

$$\{i \in I \mid \mathfrak{B}_i \models \Phi_{k_0}(fi) \in D \tag{2}$$

and thus prove the proposition. Consider the set

$$G = \{i \in I \mid \mathfrak{B}_i \models \exists v_1(\Phi_1 \wedge \ldots \wedge \Phi_k)\} \setminus (W_0 \cup \ldots \cup W_{k_0 - 1}).$$

From (1) and from the fact that $W_0 \notin D, \ldots, W_{k-1} \notin D$ we get $G \in D$. Since $m(i) \geqslant k_0$ for any $i \in G$, it follows from the construction of f that $G \subseteq \{i \in I \mid \mathfrak{B}_i \models \Phi_k(fi)\}$ and from this we obtain (2). □

Exercises

1. Show that the axioms of Boolean algebras are true in $\mathfrak{B}_n(T)$.

2. Suppose a signature Σ_0 consists of a countable set $\{r_i \mid i \in \omega\}$ of one-place predicates and a theory T_0 is defined by a set of axioms

$$\{\exists v_1(s_1(v_1) \wedge \ldots \wedge s_n(v_1)) \mid n \in \omega, \qquad s_1 \in \{r_1, \neg r_1\}, \ldots, s_n \in \{r_n, \neg\, r_n\}\}.$$

Show that T_0 is a complete theory without a universal countable model. (*Hint*. The completeness of T_0 follows from the fact that $\mathfrak{A} \upharpoonright \Sigma_1 \cong \mathfrak{B} \upharpoonright \Sigma_1$ for any finite $\Sigma_1 \subseteq \Sigma_0$ and any countable models $\mathfrak{A}$, $\mathfrak{B}$ of a theory T; that T has no universal model follows from the fact that all 1-types $\{s_i(v_1) \mid i \in \omega, s_i \in \{r_i, \neg r_i\}\}$ are compatible with T_0.)

29. CATEGORICITY

Theorem 24.3 shows that for an infinite system $\mathfrak{A}$, $\mathrm{Th}(\mathfrak{A})$ does not define $\mathfrak{A}$ (to within an isomorphism). There is, however, an interesting class of systems $\mathfrak{A}$ whose theory defines $\mathfrak{A}$ to within an isomorphism among systems of the same power. In this section we shall discuss some properties of theories of such systems. The signatures in this section have a countable or finite power.

DEFINITION. A class K of algebraic systems of a signature Σ is said to be *categorical in a power* $\varkappa$ or $\varkappa$*-categorical* if all systems in K of power $\varkappa$ are isomorphic. A theory T of Σ is said to be *categorical in* $\varkappa$ if the class $K_\Sigma(T)$ is $\varkappa$-categorical.

If a class K has no systems of power $\varkappa$, then by definition it is categorical in $\varkappa$. If K is a class of algebraic systems (T is a theory) of Σ, then by K_∞ (by T_∞) we denote the class of infinite algebraic systems of K (the theory $T \cup \{\exists v_1 \dots \exists v_n(\bigwedge_{i<j\leqslant n} \neg v_i \approx v_j) \mid n \in \omega\}$). It is clear that $K_\Sigma(T_\infty) = (K_\Sigma(T))_\infty$.

PROPOSITION 1. *If a theory T of a signature Σ is categorical in some infinite power $\varkappa$, then T_∞ is complete.*

PROOF. Let $\mathfrak{A}$ and $\mathfrak{B}$ be two infinite models of T. It suffices to show that $\mathfrak{A} \equiv \mathfrak{B}$. By Theorem 24.2 there are countable elementary subsystems $\mathfrak{A}_1 < \mathfrak{A}$ and $\mathfrak{B}_1 < \mathfrak{B}$. By Theorem 24.3 there are elementary extensions $\mathfrak{A}_2 > \mathfrak{A}_1$ and $\mathfrak{B}_2 > \mathfrak{B}_1$ of power $\varkappa$. Since $\mathfrak{A}_2$ is isomorphic to $\mathfrak{B}_2$, we have $\mathfrak{A}_2 \equiv \mathfrak{B}_2$. Hence $\mathfrak{A} \equiv \mathfrak{B}$. □

If T is complete and has finite models, then by Corollary 24.2 all models of T are isomorphic to some finite system. Up to the end of this section we let T denote a complete theory of Σ having infinite models. Notice that if T is a complete theory, then any principal compatible n-type is satisfiable in any model of T.

THEOREM 14 (Ryll-Nardzewski). *For a theory T to be categorical in a countable power it is necessary and sufficient that for any $n \in \omega$ algebras $\mathfrak{B}_n(T)$ be finite.*

PROOF. Necessity. Let $\mathfrak{B}_{n_0}(T)$ be an infinite Boolean algebra. Since T is complete, we have $|\mathfrak{B}_0(T)| = 2$ and hence $n_0 > 0$. By Proposition 12.3 there is a nonprincipal ultrafilter U on $\mathfrak{B}_{n_0}(T)$. It is clear that the n_0-type $Z = \{\Phi \in F_n(\Sigma) \mid \|\Phi\| \in U\}$ is a nonprincipal n_0-type in T. By Theorem 11 there is a countable model $\mathfrak{A}$ of T in which Z is omitted. Since $T \cup Z$ is compatible, by the theorem on the existence of a model there is a model $\mathfrak{B}$ in which Z is realized. Since $\mathfrak{B}$ may be assumed countable, T is not countably categorical.

Sufficiency. Let $\mathfrak{B}_n(T)$ be finite for all $n \in \omega$. Then any n-type Z is principal in T. By Proposition 28.4 it suffices to show that any countable model $\mathfrak{A}$ of T is saturated, to do this it is in turn sufficient to show that any 1-type of the signature $\Sigma_{\{a_1, \dots, a_n\}}$, where $a_1, \dots, a_n \in A$, is principal in $T_1 = \mathrm{Th}(\mathfrak{A}_{\{a_1, \dots, a_n\}})$. This follows from the fact that the mapping h transforming $\Phi(v_1, \dots, v_{n+1})$ into $\Phi(v_1, c_{a_1}, \dots, c_{a_n})$ preserves the relation $\|\Phi\| \leqslant \|\Psi\|$ (i. e. $T \rhd \Phi \to \Psi \Rightarrow T_1 \rhd h\Phi \to h\Psi$) and any $(n+1)$-type of Σ is principal in T. □

The following proposition has been proved by P. Lindström.

PROPOSITION 2. *If an* $\forall\exists$*-axiomatizable consistent theory* T *of* Σ *is categorical in a countable power, then* T *is model-complete.*

PROOF. We shall say that a formula $\Phi(x_1, \ldots, x_n)$ of Σ is preserved in going to submodels (supermodels) of T if for any models $\mathfrak{A} \subseteq \mathfrak{B}$ of T and any $a_1, \ldots, a_n \in A$ the truth of $\Phi(a_1, \ldots, a_n)$ in $\mathfrak{B}$ (in $\mathfrak{A}$) implies the truth of $\Phi(a_1, \ldots, a_n)$ in $\mathfrak{A}$ (in $\mathfrak{B}$). Consider a set G of formulas of Σ in prenex nf not preserved in going to submodels of T. It is clear that T is model-complete if and only if $G = \varnothing$. Suppose that T is not model-complete. We choose $\Phi_0(x_1, \ldots, x_n) \in G$ whose quantifier prefix has a least length r_0. It is obvious that $r_0 > 0$. Let $\Phi_0 = Qy\Psi_0(y, x_1, \ldots, x_n)$. It follows from the minimality of r_0 that Ψ_0 is preserved in going to subsystems and hence $Q = \exists$. Since $\neg\Psi_0$ is equivalent to a formula with a quantifier prefix of length $r_0 - 1$, it follows from the minimality of r_0 that Ψ_0 is preserved in going to supersystems.

We choose $\varphi\colon \omega \to \omega^n$ such that for any $a \in \omega^n$ the set $\{n \mid \varphi n = a\}$ is infinite. We construct a sequence $\mathfrak{A}_m$, $m \in \omega$ of countable models of T with the following properties:

(1) $A_m \subseteq \omega$ and the set $\omega \setminus A_k$ is infinite;

(2) $\mathfrak{A}_m \subseteq \mathfrak{A}_s$ for $m \leqslant s$;

(3) if $\varphi m \in (A_m)^n$ and there is a countable model $\mathfrak{B} \supseteq \mathfrak{A}_m$ of T for which $\mathfrak{B} \vDash \Phi_0(\pi_1^n(\varphi m), \ldots, \pi_n^n(\varphi m))$, then as $\mathfrak{A}_{m+1}$ we take a model of T satisfying condition (1) for $k = m + 1$ such that $\mathfrak{A}_m \subseteq \mathfrak{A}_{m+1}$ and $\mathfrak{A}_{m+1} \vDash \Phi_0(\pi_1^n(\varphi m), \ldots, \pi_n^n(\varphi m))$.

Consider a system $\mathfrak{A}_\omega = \bigcup\limits_{m \in \omega} \mathfrak{A}_m$ which is by the $\forall\exists$-axiomatizability of T a model of T (Proposition 25.4(b)). Since $\Phi_0 \in G$, there are models $\mathfrak{A} \subseteq \mathfrak{B}$ and $a_1, \ldots, a_n \in A$, $\mathfrak{B} \vDash \Phi_0(a_1, \ldots, a_n)$ and $\mathfrak{A} \vDash \neg\Phi_0(a_1, \ldots, a_n)$. By taking corresponding countable elementary subsystems it may be assumed that $\mathfrak{A}$ and $\mathfrak{B}$ are countable, and it may be assumed by the categoricity of T in a countable power that $\mathfrak{A} = \mathfrak{A}_\omega$. Since $A_\omega \subseteq \omega$, it follows from the condition on φ that $\varphi m_0 = \langle a_1, \ldots, a_n\rangle \in (A_{m0})^n$ for some $m_0 \in \omega$. Since $\mathfrak{A}_{m0} \subseteq \mathfrak{A}_\omega \subseteq \mathfrak{B}$, from property (3) we get $\mathfrak{A}_{m0+1} \vDash \Phi_0(a_1, \ldots, a_n)$ and so we have $\mathfrak{A}_{m0+1} \vDash \Psi_0(b, a_1, \ldots, a_n)$ for some $b \in \omega$. This contradicts the fact that $\mathfrak{A}_\omega \vDash \neg\exists y\Psi_0(y, a_1, \ldots, a_n)$ and that Ψ_0 is preserved in going to supersystems. □

Notice that the condition that a theory T should be $\forall\exists$-axiomatizable is also necessary in the preceding proposition for T to be model-complete. Namely, we can prove the converse of Proposition 25.4(b): if an axiomatizable class K is closed under unions of systems, then K is $\forall\exists$-axiomatizable. Any model-complete theory therefore is $\forall\exists$-axiomatizable.

The theory of densely ordered sets without the first and the last element is categorical in a countable power (Proposition 15.4) and noncategorical in no infinite uncountable power (Exercise 1). The theory of algebraically closed fields of characteristic 0 is categorical in all infinite uncountable powers and noncategorical in a countable power. It is easy to construct examples of complete theories categorical in all infinite powers and theories noncategorical in all infinite powers. As was shown by M. Morley, there are no other cases of categoricity "distinction" for complete theories of a countable signature with infinite models.

The remainder of this section will be devoted to the following theorem proved by F. A. Palyutin. Its proof uses many of the results of the present chapter and illustrates an important method of model theory, the method of minimal sets.

THEOREM 15. *If a quasi-variety K is categorical in a countable power, then it is categorical in all non-unit powers.*

A class of non-one-element systems of K is denoted by K_+. In what follows we let K be a countably categorical quasi-variety of Σ for which K_+ is not empty. Elements of classes K, K_+ and K_∞ will be called K-systems, K_+-systems and K_∞-systems respectively. Unless otherwise stated, by a formula we shall mean a formula of Σ. In what follows, unless otherwise stated, the letters $\mathfrak{A}$, $\mathfrak{B}$ will denote K-systems. By $\overline{w}$ we denote an ordered set $\langle w_1, \ldots, w_n \rangle$, writing $\overline{w} \in A$ if $w_1, \ldots, w_n \in A$ and $\Phi(\overline{w})$ instead of $\Phi(w_1, \ldots, w_n)$. If $\Phi(y, \overline{x})$ is a formula, $\overline{a} \in A$, then $\Phi(\mathfrak{A}, \overline{a})$ denotes a set $\{b \in A \mid \mathfrak{A} \models \Phi(b, \overline{a})\}$. If $t(y_1, \ldots, y_m, \overline{x})$ is a term, $\overline{a} \in A$ and $X_1 \subseteq A, \ldots, X_m \subseteq A$, then $t^{\mathfrak{A}}(X_1, \ldots, X_m, \overline{a})$ denotes a set

$$\{b_0 \in A \mid \text{there are } b_1 \in X_1, \ldots, b_m \in X_m \text{ such that}$$
$$b_0 = t^{\mathfrak{A}}(b_1, \ldots, b_m, \overline{a})\}.$$

If $X_1 = \ldots = X_m = X$, then we write $t^{\mathfrak{A}}(\bar{X}, \bar{a})$ instead of $t^{\mathfrak{A}}(X_1, \ldots, X_n, \bar{a})$. To abbreviate the notation we shall often leave out universal quantifiers in writing quasi-identities, i. e. denote a quasi-identity $\forall x_1 \ldots \forall x_n \Phi(x_1, \ldots, x_n)$ by $\Phi(x_1, \ldots, x_n)$. For notational simplicity we shall also identify "diagonal" elements $f_a \in A^I$ identically $a \in A$ on I with an element $a \in A$. A system $\mathfrak{A}$ will therefore be assumed to be a subsystem of its Cartesian power $\mathfrak{A}^I$. This is possible because the mapping assigning to an element $a \in A$ an element $f_a \in A^I$ is an isomorphism of $\mathfrak{A}$ onto a subsystem of diagonal elements of $\mathfrak{A}^I$.

By Propositions 1 and 2 a theory $\mathrm{Th}(K_\infty)$ is complete and model-complete. It follows from Propositions 25.4 (a) and 25.5 (a) that a class K is closed under subsystems and Cartesian products. In particular, $K_+ \neq \varnothing$ implies $K_\infty \neq \varnothing$.

LEMMA 1. (a) *If a sentence conditionally filters together with its negation* $\neg\Phi$ *and is true on some* K_+*-system* $\mathfrak{A}$, *then it is true on any* K_+*-system. Filtering sentences and quasi-identities conditionally filter together with their negations.*

(b) *For any* K*-system* $\mathfrak{A}$ *and any finite set* $X \subseteq A$ *the system* $\mathfrak{A}(X)$ *is finite.*

PROOF. (a) If a sentence Φ is false in a K_+-system $\mathfrak{B}$, then it follows from the conditional filtration of Φ and $\neg\Phi$ that Φ is true in $\mathfrak{A}^\omega$ and false in $\mathfrak{B}^\omega$. This contradicts the fact that $\mathrm{Th}(K_\infty)$ is complete. If Φ is a filtering formula, then it is obvious that $\neg\Phi$ conditionally filters. The conditional filtration of a quasi-identity is shown in the proof of Proposition 25.5(a). The negation of a quasi-identity Φ is equivalent to a sentence $\exists x_1 \ldots \exists x_n(\Phi_1 \wedge \neg\Phi_2)$, where Φ_1, Φ_2 are filtering formulas. By Lemma 17.2 $\neg\Phi$ conditionally filters.

(b) Let $\mathfrak{A}(a_1, \ldots, a_n)$ be infinite. For every $a \in A\ (a_1, \ldots, a_n)$ there is a term $t_a(v_1, \ldots, v_n)$ such that $t_a^{\mathfrak{A}}(a_1, \ldots, a_n) = a$. Then formulas $v_{n+1} \approx t_a(v_1, \ldots, v_n)$, $a \in A(a_1, \ldots, a_n)$ are pairwise nonequivalent in $\mathrm{Th}(\mathfrak{A}(a_1, \ldots, a_n)) = \mathrm{Th}(K_\infty)$. Since $\mathrm{Th}(K_\infty)$ is ω-categorical, this contradicts Theorem 14. □

LEMMA 2. *If* $\Phi(y, \bar{x})$ *is a filtering formula,* $\mathfrak{A} \in K_+$, $\bar{a} = \langle a_1, \ldots, a_n \rangle \in A$ and $\Phi(\mathfrak{A}, \bar{a})$ *contains at least two elements, then*

(a) *there is a term* $t(\bar{y}, \bar{x})$ *such that* $t^{\mathfrak{A}}(\overline{\Phi(\mathfrak{A}, \bar{a})}, \bar{a}) = A$;

(b) *for any* $\mathfrak{B} \in K_+$ *and* $\bar{b} = \langle b_1, \dots, b_n \rangle \in B$ *a set* $\Phi(\mathfrak{B}, \bar{b})$ *contains at least two elements or is empty.*

PROOF. (a) We first prove that if $\Phi(\mathfrak{A}, \bar{a})$ is infinite, then the set $X = \Phi(\mathfrak{A}, \bar{a}) \cup \{a_1, \dots, a_n\}$ generates $\mathfrak{A}$. Let $\{t_i(v_1, \dots, v_i) \mid i \in \omega\}$ be the enumeration of all terms. For each $i \in \omega$, $i \geqslant n$, consider a formula

$$\Psi_i(v_0, v_1, \dots, v_n) = \exists v_{n+1} \exists v_{n+2} \dots$$
$$\dots \exists v_i \Big(\bigvee_{j \leqslant i} v_0 \approx t_j \wedge \bigwedge_{n < k \leqslant i} \Phi(v_k, v_1, \dots, v_n)\Big)$$

whose truth on a system $\mathfrak{B}$ for an interpretation $\gamma \colon \{v_0, \dots, v_n\} \to B$ is equivalent to the fact that $\gamma(v_0)$ is the value of a term $t_j^{\mathfrak{B}}(\gamma(v_1), \dots, \gamma(v_n), b_{n+1}, \dots, b_j)$, where $j \leqslant i$ and $b_{n+1}, \dots, b_i \in \Phi(\mathfrak{B}, \gamma(v_1), \dots, \gamma(v_n))$. It is clear that for any $b \in A(X)$ there is $i \in \omega$, $i \geqslant n$, for which $\mathfrak{A}(X) \vDash \Psi_i(b, \bar{a})$. By Theorem 14 there is a finite set $\{i_1, \dots, i_k\}$ such that for any $i \in \omega$ $\mathrm{Th}(K_\infty) \rhd \Psi_i \to (\Psi_{i_1} \vee \dots \vee \Psi_{i_k})$. Hence $\forall v_0 (\Psi_{i_1}(v_0, \bar{a}) \vee \dots \vee \Psi_{i_k}(v_0, \bar{a}))$ is true in $\mathfrak{A}(X)$. Since $\mathfrak{A}(X) \prec \mathfrak{A}$, that formula is true in $\mathfrak{A}$ from which it follows that $\mathfrak{A}$ is generated by the set X. Suppose that (a) is false. Then there are $b_i \in A$, $n \leqslant i \in \omega$ such that $t_i^{\mathfrak{A}}(\bar{a}, a_{n+1}, \dots, a_i) \neq b_i$ for any $a_{n+1}, \dots, a_i \in \Phi(\mathfrak{A}, \bar{a})$. Then the set $Y = \Phi(\mathfrak{A}^\omega, \bar{a}) = (\Phi(\mathfrak{A}, a))^\omega$ is infinite and $g \notin A^\omega(Y \cup \{a_1, \dots, a_n\})$, where $gi = b_i$, $i \in \omega$. This contradicts the foregoing.

(b) Suppose that there are $\mathfrak{B} \in K_+$ and $\bar{b} \in B$ such that $\Phi(\mathfrak{B}, \bar{b}) = \{d_0\}$. Since Φ is a filtering formula, the set $\Phi(\mathfrak{A} \times \mathfrak{B}, \bar{a} \times \bar{b})$ is equal to $\Phi(\mathfrak{A}, \bar{a}) \times \{d_0\}$, where $\bar{a} \times \bar{b} = \langle \langle a_1, b_1 \rangle, \dots, \langle a_n, b_n \rangle \rangle$. Let $a_0 \in A$; $d_1, d_2 \in B$, $d_1 \neq d_2$. Then by (a) we have

$$t(\langle c_1, d_0 \rangle, \dots, \langle c_m, d_0 \rangle, \bar{a} \times \bar{b}) = \langle a_0, d_1 \rangle \quad \text{and}$$
$$t(\langle c_1', d_0 \rangle, \dots, \langle c_m', d_0 \rangle, \bar{a} \times \bar{b}) = \langle a_0, d_2 \rangle$$

for some term $t(y_1, \dots, y_m, \bar{x})$ and some $c_1, \dots, c_m, c_1', \dots, c_m' \in \Phi(\mathfrak{A}, \bar{a})$. From the definition of the operations on $\mathfrak{A} \times \mathfrak{B}$ we get $t(d_0, \dots, d_0, \bar{b}) = d_1$ from the first equation and $t(d_0, \dots, d_0, \bar{b}) = d_2$ from the second, which contradicts the condition $d_1 \neq d_2$. □

Consider the maximal Th(K)-compatible set

$$X^* = \{\neg v_1 \approx v_2\} \cup \{\Phi_i(v_1, v_2) \mid i \in \omega\},$$

where $\Phi_i(v_1, v_2)$, $i \in \omega$, are atomic formulas. Let a signature Σ^* be obtained from Σ by adding two new constants, c_1 and c_2. Consider the quasi-variety K^* of Σ^* whose set of axioms consists of the axioms of K as well as of quasi-identities $v_1 \approx v_1 \rightarrow \Phi(c_1, c_2)$ for atomic formulas $\Phi(v_1, v_2) \in X^*$ and of quasi-identities $\Phi(c_1, c_2) \rightarrow v_1 \approx v_2$ for atomic $\Phi(v_1, v_2) \notin X^*$.

LEMMA 3. (a) *For any K_+-system $\mathfrak{A}$ there is a K^*-system $\mathfrak{A}^*$ such that $\mathfrak{A}^* \upharpoonright \Sigma = \mathfrak{A}$.*

(b) *The quasi-variety K^* is categorical in a countable power.*

PROOF. Since X^* is maximal, it suffices to show that X^* is satisfiable in any K_+-system $\mathfrak{A}$. It follows from Theorem 14 that there is $n_0 \in \omega$ such that Th$(K_\infty) \vartriangleright (\Phi_0 \wedge \ldots \wedge \Phi_{n_0}) \rightarrow \Phi_i$ for all $i \in \in \omega$. Since $K_\infty \neq \varnothing$, by Lemma 1 (a) $\mathfrak{A} \models (\Phi_0 \wedge \ldots \wedge \Phi_{n_0}) \rightarrow \Phi_i$ for all $i \in \omega$. Therefore it suffices to show that the sentence $\exists v_1 \exists v_2 \Psi(v_1, v_2)$, where $\Psi(v_1, v_2)$ is equal to $\neg v_1 \approx v_2 \wedge \Phi_0 \wedge \ldots \ldots \wedge \Phi_{n_0}$, is true in $\mathfrak{A}$. Let X^* be satisfiable in a K-system $\mathfrak{B}$. Then $|B| > 1$ and $\exists v_1 \exists v_2 \Psi(v_1, v_2)$, is true in a K_∞-system $\mathfrak{B}^\omega$. Since Th(K_∞) is complete, we have $\mathfrak{A}^\omega \models \Psi(f_1, f_2)$ for some $f_1, f_2 \in A^\omega$. Since $\mathfrak{A}^\omega \models \neg f_1 \approx f_2$, we have $f_1 i_0 \neq f_2 i_0$ for some $i_0 \in \omega$. From the filtration of $\Phi_0 \wedge \ldots \wedge \Phi_{n_0}$ we get $\mathfrak{A} \models \Psi(f_1 i_0, f_2 i_0)$.

(b) As was shown in the proof of Theorem 14, every countable K_∞-system is saturated. Since any K^*_∞-system $\mathfrak{A}^*$ is an expansion of some K_∞-system $\mathfrak{A}$ by two constants, $\mathfrak{A}^*$ is saturated. By Proposition 28.4 therefore it suffices to show that any K^*_∞-systems $\mathfrak{A}$, $\mathfrak{B}$ are elementarily equivalent. Let $\nu^{\mathfrak{A}}(c_1) = a_1$, $\nu^{\mathfrak{A}}(c_2) = a_2$, $\nu^{\mathfrak{B}}(c_1) = b_1$ and $\nu^{\mathfrak{B}}(c_2) = b_2$. Since quasi-identities $\Phi(c_1, c_2) \rightarrow v_1 \approx v_2$ are equivalent to the sentence $\neg \Phi(c_1, c_2)$ in Th(K^*_+), it follows from the axioms of K^* that a mapping assigning to elements a_1, a_2 elements b_1, b_2 respectively is extended to an isomorphism $f \colon \mathfrak{A}_0 \simeq \mathfrak{B}_0$, where $\mathfrak{A}_0 = \mathfrak{A}(a_1, a_2) \upharpoonright \Sigma$ and $\mathfrak{B}_0 = \mathfrak{B}(b_1, b_2) \upharpoonright \Sigma$. Then f is extended to an isomorphism of K_∞-systems $\mathfrak{A}_0^\omega \subseteq \mathfrak{A}^\omega \upharpoonright \Sigma$ and $\mathfrak{B}_0^\omega \subseteq \mathfrak{B}^\omega \upharpoonright \Sigma$. Hence $\langle \mathfrak{A}_0^\omega, a_1, a_2 \rangle \equiv \langle \mathfrak{B}_0^\omega, b_1, b_2 \rangle$ and from the model completeness of Th(K_∞) we get $\langle \mathfrak{A}^\omega \upharpoonright \Sigma, a_1, a_2 \rangle \equiv \langle \mathfrak{B}^\omega \upharpoonright \Sigma, b_1, b_2 \rangle$. The model completeness of Th(K_∞) also implies that $\langle \mathfrak{A} \upharpoonright \Sigma, a_1, a_2 \rangle \equiv \langle \mathfrak{B} \upharpoonright \Sigma, b_1, b_2 \rangle$ and hence $\mathfrak{A} \equiv \mathfrak{B}$. □

In what follows it is assumed that the signature Σ con ains the constants c_1, c_2 and that the sentence $\neg c_1 \approx c_2$ is true in any K_+-system. Such an assumption for the proof of Theorem 15 may be made by Lemma 3. In this way we define for any K_+-system a K_+-system $\mathfrak{A}(\varnothing)$ whose carrier consists of the values in $\mathfrak{A}$ of the constant terms. It follows from Lemma 1(a) that $\mathfrak{A}(\varnothing) \simeq \mathfrak{B}(\varnothing)$ for any K_+-systems $\mathfrak{A}$ and $\mathfrak{B}$. A set $X \subseteq A$ is said to be atomically minimal in a K-system $\mathfrak{A}$ if $|X| > 1$ and for any atomic formula $\Phi(y, \bar{x})$, any $\bar{a} \in A$ the set $X \cap \Phi(\mathfrak{A}, \bar{a})$ is empty, one-element or equal to X.

LEMMA 4. *There is a filtering formula $\Phi^*(v_1)$ such that for any K_+-system $\mathfrak{A}$ the set $\Phi^*(\mathfrak{A})$ is atomically minimal in $\mathfrak{A}$.*

PROOF. Let $\mathfrak{B} \in K_+$. By Lemma 1 (b) a K_+-system $\mathfrak{B}_0 = \mathfrak{B}(\varnothing)$ is finite. Consider a conjunction $\Phi^*(v_1)$ of atomic formulas such that $|\Phi^*(\mathfrak{B}_0)| > 1$ and for any atomic formula $\Phi(v_1)$ the set $\Phi^*(\mathfrak{B}_0) \cap \Phi(\mathfrak{B}_0)$ is empty, one-element or equal to $\Phi^*(\mathfrak{B}_0)$. Let $\Phi(y, \bar{x})$ be an atomic formula. Since any element $b \in B_0$ is the value in $\mathfrak{B}_0$ of a constant term, the set $\Phi^*(\mathfrak{B}_0) \cap \Phi(\mathfrak{B}_0, \bar{b})$ is empty, one-element or equal to $\Phi^*(\mathfrak{B}_0)$ for any $\bar{b} \in B_0$. By Lemma 2(b) there are no $\bar{a}, \bar{b} \in B_0$ such that $\Phi^*(\mathfrak{B}_0) \subseteq \Phi(\mathfrak{B}_0, \bar{b})$ and $\Phi^*(\mathfrak{B}_0) \cap \cap \Phi(\mathfrak{B}_0, \bar{a})$ is one-element. Thus one of the following quasi-identities is true in $\mathfrak{B}_0$:

(a) $(\Phi^*(v_1) \wedge \Phi(v_1, \bar{x}) \wedge \Phi^*(v_2) \wedge \Phi(v_2, \bar{x})) \to v_1 \approx v_2$;

(b) $(\Phi^*(v_1) \wedge \Phi(v_1, \bar{x}) \wedge \Phi^*(v_2)) \to \Phi(v_2, \bar{x})$.

By Lemma 1 (a) one of these is true in any K_+-system $\mathfrak{A}$. Since $\Phi^*(\mathfrak{A}) \supseteq \Phi^*(\mathfrak{A}(\varnothing))$ and $\mathfrak{A}(\varnothing) \simeq \mathfrak{B}_0$, we have $|\Phi^*(\mathfrak{A})| > 1$. Hence $\Phi^*(\mathfrak{A})$ is atomically minimal in $\mathfrak{A}$. □

Let $\mathfrak{A} \in K_+$. A set $X \subseteq \Phi^*(\mathfrak{A})$ is said to be a basis for $\mathfrak{A}$ if the following conditions hold:

(1) $\mathfrak{A}(X) = \mathfrak{A}$;

(2) if $a_1, \ldots, a_n$ are pairwise distinct elements of X and $\mathfrak{A} \vDash \vDash \Phi(a_1, \ldots, a_n)$ for some atomic formula $\Phi(v_1, \ldots, v_n)$, then the quasi-identity $(\Phi^*(v_1) \wedge \ldots \wedge \Phi^*(v_n)) \to \Phi(v_1, \ldots, v_n)$ is true in any K_+-system.

LEMMA 5. (a) *If $\Phi(y, \bar{x})$ is a filtering formula and $\Phi(\mathfrak{A}, \bar{a}) = \{b\}$ for a K_+-system $\mathfrak{A}$ and $\bar{a} \in A$, then $t^{\mathfrak{A}}(\bar{a}) = b$ for some term $t(\bar{x})$.*

(b) *Every K_+-system $\mathfrak{A}$ has a basis.*

PROOF. Let $\mathfrak{A}_0 = \mathfrak{A}(\bar{a})$. If (a) does not hold, then the sentence $\exists y \Phi(y, \bar{a})$ is false in the K_∞-system $\mathfrak{A}_0^\omega$ and true in $\mathfrak{A}^\omega \supseteq \mathfrak{A}_0^\omega$. This contradicts the model completeness of $\mathrm{Th}(K_\infty)$.

(b) Let $X \subseteq \Phi^*(\mathfrak{A})$ be a maximal set satisfying condition (2). By Lemma 2(a) it suffices to show that $\mathfrak{A}(X)$ contains $\Phi^*(\mathfrak{A})$. Suppose that there is $a_0 \in \Phi^*(\mathfrak{A}) \setminus A(X)$. Let $\mathfrak{A} \models \Phi(a_0, a_1, \ldots, a_n)$ for an atomic $\Phi(v_0, v_1, \ldots, v_n)$ and pairwise distinct $a_1, \ldots, a_n \in X$. By (a) and the atomical minimality of $\Phi^*(\mathfrak{A})$ we have $\Phi^*(\mathfrak{A}) \subseteq \Phi(\mathfrak{A}, a_1, \ldots, a_n)$. Since $\Phi^*(\mathfrak{A}(\varnothing)) \neq \varnothing$, we have $\mathfrak{A} \models \Phi^*(t_0) \wedge \Phi(t_0, a_1, \ldots, a_n)$ for some constant term t_0. Since X satisfies condition (2) and $\Phi^*(t_0) \in \mathrm{Th}(K_+)$ (Lemma 1(a)), the set $\Phi^*(\mathfrak{B}) \wedge \Phi(\mathfrak{B}, b_1, \ldots, b_n)$ is not empty for any K_+-system $\mathfrak{B}$ and any $b_1, \ldots, b_n \in \Phi^*(\mathfrak{B})$. It follows from Lemma 2(b) therefore that if $|\Phi(\mathfrak{A}, a_1, \ldots, a_n) \cap \Phi^*(\mathfrak{A})| > 1$ and $\Phi^*(\mathfrak{B})$ is atomically minimal, then $\Phi(b_0, b_1, \ldots, b_n)$ is true in any K_+-system $\mathfrak{B}$ for any $b_0, b_1, \ldots, b_n \in \Phi^*(\mathfrak{B})$. Hence $X \cup \{a_0\}$ satisfies condition (2), which contradicts the minimality of X. □

PROOF OF THEOREM 15. Let $\mathfrak{A}$, $\mathfrak{B}$ be two K_+-systems of the same power $\varkappa$ and let X, Y be their bases. It follows from the definition of a basis that any distinct-valued mapping $f\colon X \to Y$ is extended in a natural way to an isomorphism of $\mathfrak{A}$ onto $\mathfrak{B}(f(X))$. By property (1) of a basis therefore it suffices to notice that $|X| = |Y|$. If $\varkappa \geqslant \omega$, then from Lemma 1(b) we get $|X| = |Y| = \varkappa$. If $\varkappa < \omega$ and $|X| \leqslant |Y|$, then $\mathfrak{A}$ is isomorphic to a subsystem $\mathfrak{B}_1 \subseteq \mathfrak{B}$. Since $|B_1| = |A| = |B|$, we have $\mathfrak{B}_1 = \mathfrak{B}$. □

Exercises

1. Show that a theory T_0 of dense linear orderings without the first and the last element is categorical in no infinite uncountable power. (*Hint.* Suppose $\mathfrak{A}$ is a model of T_0 of power $\varkappa > \omega$ and $\mathfrak{A}_0$ is a countable model of T_0 for which $A_0 \cap A = \varnothing$; consider a model $\mathfrak{A}_1$ with carrier A^2 and relation $\langle a, b\rangle \leqslant^{\mathfrak{A}_1} \langle c, d\rangle \Leftrightarrow (a <^{\mathfrak{A}} c$ or $(a = c$ and $b \leqslant^{\mathfrak{A}} d))$ and a model $\mathfrak{A}_2$ with carrier $A \cup A_0$ and relation

$$a \leqslant^{\mathfrak{A}_2} b \Leftrightarrow ((a \in A \text{ and } b \in A_0) \text{ or } (a, b \in A \text{ and } a \leqslant^{\mathfrak{A}} b) \text{ or } (a, b \in A_0 \text{ and } a \leqslant^{\mathfrak{A}_0} b));$$

then $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are nonisomorphic.)

2. Show that a variety of Boolean algebras is categorical in all finite powers and noncategorical in all infinite powers.

3. Prove that a variety M with the axioms (universal quantifiers omitted)
(1) $f(g_1(x), g_2(x)) \approx x$,
(2) $f(x, y) \approx f(g_1(x), g_2(y))$,
(3) $g_1(f(g_1(x), g_1(y))) \approx g_1(x)$,
(4) $g_2(f(g_1(x), g_1(y))) \approx g_1(y)$,
(5) $g_i(g_k(x)) \approx g_k(x)$, $i, k \in \{1, 2\}$
is categorical in all powers. (*Hint*. Show that $\nu^{\mathfrak{A}}(f)$ for any $\mathfrak{A} \in M$ is a distinct-valued mapping of $(g_1^{\mathfrak{A}}[A])^2$ onto A^2 and that any distinct-valued mapping h: $g_1^{\mathfrak{A}}[A] \to g_1^{\mathfrak{B}}[B]$ for any $\mathfrak{A}, \mathfrak{B} \in M$ is extended to an isomorphism of a system $\mathfrak{A}$ onto $\mathfrak{B}(h(g_1^{\mathfrak{A}}[A]))$ transforming a into $f^{\mathfrak{B}}(hg_1^{\mathfrak{A}}(a), hg_2^{\mathfrak{A}}(a))$.)

4. Construct an example showing that one cannot state in Theorem 15 that K is also categorical in power 1.

5. Generalize Proposition 2 to theories categorical in an infinite power $\varkappa$ and thus obtain the Lindström theorem in full extent. (*Hint*. Use the method of Proposition 2, with ω replaced by $\varkappa$, and show that if the formula Φ is not preserved in going to the submodels of a theory T, then Φ is not preserved in going to submodels of a power $\varkappa$.)

Chapter 6

PROOF THEORY

30. THE GENTZEN SYSTEM *G*

The calculi studied earlier are natural formalizations of the rules of logic. For a deeper study of the very concept of proof other forms of calculi are more convenient. In this section we shall study one of such calculi, *G*, similar to the calculus proposed by Gentzen.

The alphabet of the calculus *G* differs from that of the calculus of predicates of Chapter 4 in that it has no implication sign and no equality sign. It is assumed in this and further sections (up to Sec. 33) that the signature of *G* is arbitrary but fixed. In Sec. 33 the signature of *G* will be extended by adding some new function symbols. Bearing this in mind, no references will be made to the signature of *G*. The definition of the notion of a *formula* of *G* differs from the definition of a formula in Sec. 16 in that (1) point 2 of that definition is missing (it concerns the equality sign $\approx$), (2) in point 3 of the definition of a formula the case $(\Phi \rightarrow \Psi)$ is left out and (3) it is required of a formula that it should have the property that its variables are unmixed. This last property is defined as follows: a formula of the calculus of predicates satisfies the condition that it should have unmixed variables if any variable of a formula Φ has either only free or only bound occurrences in Φ. Sequents of *G* are expressions of the form $\Gamma \vdash \Theta$, where Γ and Θ are arbitrary finite sequences of formulas of *G* and for the sequence Γ, Θ the condition that the variables should be unmixed, formulated similarly to the condition that the variables of formulas should be unmixed, holds. The conventions about abbreviating the notation of formulas and some of the symbols used below have the same meaning as in Chapter 4.

DEFINITION. *Axioms of G* are sequents of the form $\Phi, \Gamma \vdash \Theta, \Phi$, where Φ is an atomic formula, Γ and Θ are sequences (possibly empty) of atomic formulas.

DEFINITION. *Rules of inference of G* are the following:

$$1.\ \frac{\Gamma \vdash \Theta, \Phi \quad \Gamma \vdash \Theta, \Psi}{\Gamma \vdash \Theta, \Phi \wedge \Psi}, \qquad 2.\ \frac{\Phi, \Psi, \Gamma \vdash \Theta}{\Phi \wedge \Psi, \Gamma \vdash \Theta},$$

$$3.\ \frac{\Gamma \vdash \Theta, \Phi, \Psi}{\Gamma \vdash \Theta, \Phi \vee \Psi}, \qquad 4.\ \frac{\Phi, \Gamma \vdash \Theta \quad \Psi, \Gamma \vdash \Theta}{\Phi \vee \Psi, \Gamma \vdash \Theta},$$

$$5.\ \frac{\Phi, \Gamma \vdash \Theta}{\Gamma \vdash \Theta, \neg\Phi}, \qquad 6.\ \frac{\Gamma \vdash \Theta, \Phi}{\neg\Phi, \Gamma \vdash \Theta},$$

$$7.\ \frac{\Gamma \vdash \Theta, (\Phi)^x_t}{\Gamma \vdash \Theta, \exists x\Phi}, \qquad 8.\ \frac{[\Phi]^x_y, \Gamma \vdash \Theta}{\exists x\Phi, \Gamma \vdash \Theta},$$ where y does not occur free in the formulas of Γ, Θ;

$$9.\ \frac{\Gamma \vdash \Theta, [\Phi]^x_y}{\Gamma \vdash \Theta, \forall x\Phi},$$ where y does not occur free in the formulas of Γ, Θ;

$$10.\ \frac{(\Phi)^x_t, \Gamma \vdash \Theta}{\forall x\Phi, \Gamma \vdash \Theta}, \qquad 11.\ \frac{\Gamma \vdash \Delta, \Phi, \Psi, \Theta}{\Gamma \vdash \Delta, \Psi, \Phi, \Theta},$$

$$12.\ \frac{\Gamma, \Phi, \Psi, \Delta \vdash \Theta}{\Gamma, \Psi, \Phi, \Delta \vdash \Theta}, \qquad 13.\ \frac{\Gamma \vdash \Theta, \Phi, \Phi}{\Gamma \vdash \Theta, \Phi},$$

$$14.\ \frac{\Phi, \Phi, \Gamma \vdash \Theta}{\Phi, \Gamma \vdash \Theta}.$$

Rules 1 to 10 are called *basic* and Rules 11 to 14 are *structural*. The *notion of* (linear and tree form) *proof* (*derivation*, *quasi-derivation*) is defined as for the calculus of predicates.

Note some features of this calculus. One is a large symmetry of right and left hand sides of the sequent $\Gamma \vdash \Theta$ (called the *conclusion* or *succeedent* (Θ) and a *hypothesis* or *antecedent* (Γ) respectively). Second, (unlike the structural rules) each basic rule contains below the line a more complicated formula obtained from the formulas of the hypothesis (this formula will be called the *principal formula* of the rule). The third property, that of being a subformula, involves new concepts.

We define an operation l on occurrences I of sequents in a tree of sequents D as follows: if I is a final occurrence in D, then $l(I) = I$; if I is contained in a passage P above the line, then $l(I)$ is an occurrence of a sequent in the passage P below the line ($l(I)$ is the lower sequent of the passage P). If D is a tree form proof, then we define an operation s on occurrences J of formulas in D as follows: if J is contained in an occurrence I of sequents in D, then $s(J)$ occurs in a sequent $l(I)$; if J occurs in a sequence Γ or Θ (or Δ) of a sequent I, then $s(J)$ is equal to the same occurrence of a formula in Γ or Θ (or Δ), but this time in the sequent $l(I)$; for the basic rules, if J does not occur in Γ or Θ, then $s(J)$ is the principal formula of the corresponding passage; for the structural rules, if J does not occur in Γ (Θ or Δ), then in the symbols of Rules 11 to 14 we have $s(\Phi) = \Phi$, $s(\Psi) = \Psi$. If for some positive n we have $l^n(I_1) = \underbrace{l(\ldots l(I_1)\ldots)}_{n \text{ times}} = I_2$, then we say that the occurrence I_1 in a tree D is above the occurrence I_2 (and I_2 is below I_1). If for occurrences J_1 and J_2 of formulas in a proof and a positive n we have $s^n(J_1) = J_2$, then we say that J_1 is the *ancestor* of J_2 and that J_2 is a *descendant* of J_1.

If Φ is a formula of the calculus G, x is a variable, t is a term, then we shall say that the term t is free for the variable x in the formula Φ if Φ has no free occurrences of the variable x or if no variable of the term t has bound occurrences in Φ. If t is free for x in Φ, then the condition on the notation $(\Phi)^x_t$ holds and the formula $(\Phi)^x_t$ is a formula of G.

We introduce the notion of generalized subformula by defining inductively for every formula Φ of G a set $GS(\Phi)$ of generalized subformulas of the formula Φ as follows:

(1) if Φ is an atomic formula, then $GS(\Phi) = \{\Phi\}$;

(2) if $\Phi = \neg\Psi$, then $GS(\Phi) = \{\Phi\} \cup GS(\Psi)$;

(3) if $\Phi = \Phi_0 \tau \Phi_1$ ($\tau \in \{\vee, \wedge\}$), then $GS(\Phi) = \{\Phi\} \cup \cup\, GS(\Phi_0) \cup GS(\Phi_1)$;

(4) if $\Phi = Qx\Psi (Q \in \{\forall, \exists\})$, then $GS(\Phi) = \{\Phi\} \cup \cup \cup\, \{GS((\Psi)^x_t) \mid t \text{ is free for } x \text{ in } \Psi\}$.

Remark. If Ψ is a generalized subformula of a formula Φ (i. e. $\Psi \in GS(\Phi)$) and a variable v has a bound occurrence in Ψ, then it has a bound occurrence in Φ too.

The following property of being a *subformula is true*:

LEMMA 1. *The ancestor-descendant relation satisfies the following conditions: if an occurrence I_0 of a sequent is above an occurrence I_1 in a proof D, then for any occurrence of a formula in I_0 there is its only descendant in I_1; for any occurrence of a for-*

mula in I_1 *there is at least one of its ancestors in* I_0. *Any ancestor is a generalized subformula of the descendant.*

PROOF. The validity of the lemma is easy to prove by induction. □

Although in the definition of the concepts of formula and sequent of G it was required that the variables should be unmixed, this was not required in the definition of a (tree form) proof. Nevertheless it may be assumed without loss of generality that this condition holds in proofs. We may go even further. We shall say that a (tree form) proof D possesses the *property of the purity of variables* if the condition that the variables should be unmixed holds for the tree D and if for any passage in D corresponding to Rule 8 or 9 the corresponding variable y occurs only in the sequents above the lower sequent of that passage.

LEMMA 2. *For any provable sequent of G there is a proof of that sequent with the property of the purity of variables.*

The proof makes use of a "rearrangement" of a given proof of a sequent into a proof with the property of the purity of variables which consists in replacing the "subtrees" of the proof by other trees. The concept of *subtree* of a tree of sequents is defined inductively. If D consists of a single sequent, then D is itself its only subtree. If D has the form:

$$\frac{D_0, \dots, D_n}{C},$$

then the subtrees of D are: the tree D itself and all the subtrees of the trees D_0, ..., D_n. The subtrees of the tree D are in a natural one-to-one correspondence with the occurrences of the sequents in the tree D.

Notice that two different subtrees of a tree D may not differ as trees, which can be seen from the example of the tree

$$\frac{\Phi \vdash \Phi \quad \Phi \vdash \Phi}{\Phi \vdash \Phi \wedge \Phi}$$

Let us turn directly to the proof of Lemma 2. Let D be a proof of a sequent C in G. We shall say that a *variable y vanishes in a passage P* of D if y has at least one free occurrence in the sequent above the line and has no free occurrences in the sequent below the line of that passage. Notice that a variable may vanish in a passage provided that passage corresponds to one of the rules, 7 to 10. We shall say that a *variable y vanishes properly* if y vanishes in some passage and has occurrences in D only in the sequents above the lower sequent of that passage. Note that if a variable y vanishes properly, then it has only free occurrences in the tree D. If all vanishing variables in D vanish properly, then D possesses the property of the purity of variables. If D has improper vanishings of variables, then we consider a passage P in which some variable y vanishes improperly; let D' be a subtree of D corresponding to the lower sequent of that passage. We choose a variable z different from all the variables of D and replace in D the subtree D' by a subtree $[D']^y_z$ which is obtained from D' by replacing each occurrence of a formula Ψ in the occurrence of the formula $[\Psi]^y_z$. It is easily checked that the resulting tree D^* remains a proof and a proof such that the variable z vanishes in D^* properly. Induction on the number of improper vanishings shows that in a finite number of such transformations we obtain a proof (of the very same final sequent) in which all the vanishings of variables are proper. □

The following lemma allows a useful admissible rule (the rule of revision) to be introduced in the calculus G.

LEMMA 3. *If* $\Gamma \vdash \Theta$ *is a provable sequent and* Φ *is a formula such that* $\Phi, \Gamma \vdash \Theta$ *is a sequent of* G, *then the sequents* $\Phi, \Gamma \vdash \Theta$ *and* $\Gamma \vdash \Theta, \Phi$ *are provable in* G.

PROOF. Let $x_0, \ldots, x_n$ be all free variables of the formula Φ. Let D be a proof of the sequent $\Gamma \vdash \Theta$ with the property of the purity of variables. As is seen from the proof of Lemma 2, it may be assumed that all the vanishing variables of D are different from $x_0, \ldots, x_n$.

We prove the lemma by induction on the construction of the formula Φ. If Φ is an atomic formula and (D, Φ) is a tree obtained by replacing each occurrence of a sequent $\Delta \vdash \Lambda$ by an occurrence of a sequent $\Delta, \Phi \vdash \Lambda$, then (under the above assumptions about a proof D) the tree (D, Φ) is a proof of the sequent $\Gamma, \Phi \vdash \Theta$. Applying the structural rule of interchange 12 several times we obtain a proof of the sequent $\Gamma \vdash \Theta, \Phi$. Similarly defined is the tree (Φ, D) ($\Delta \vdash \Lambda$ is replaced by $\Delta \vdash \Phi, \Lambda$) which is a proof of the sequent $\Gamma \vdash \Phi, \Theta$; we use Rule 11 to complete it to the proof of the sequent $\Gamma \vdash \Theta, \Phi$.

Let $\Phi = \Phi_0 \vee \Phi_1$. By induction the provability of $\Gamma \vdash \Theta$ yields the provability of $\Phi_0, \Gamma \vdash \Theta$ and $\Phi_1, \Gamma \vdash \Theta$. Hence the following quasi-derivations:

$$\frac{\Phi_0, \Gamma \vdash \Theta \quad \Phi_1, \Gamma \vdash \Theta}{\Phi_0 \vee \Phi_1, \Gamma \vdash \Theta} \qquad \frac{\Gamma \vdash \Theta, \Phi_0, \Phi_1}{\Gamma \vdash \Theta, \Phi_0 \vee \Phi_1}$$

justify the provability of $\Phi_0 \vee \Phi_1, \Gamma \vdash \Theta$ and $\Gamma \vdash \Theta, \Phi_0 \vee \Phi_1$. The verification of the statement for $\Phi = \Phi_0 \wedge \Phi_1$ and $\Phi = \neg \Phi_0$ is similar. For formulas of the form $\Phi = \exists x\Psi(\forall x\Psi)$ we choose a variable y without occurrences in the formulas $\exists x\Psi$, $\Gamma \vdash \Theta$ and apply the induction hypothesis to the formula $[\Phi]^x_y$. As illustration, the provability of $\Gamma \vdash \Theta$ then implies the provability of $[\Phi]^x_y$, $\Gamma \vdash \Theta$ and the quasi-derivation

$$\frac{[\Phi]^x_y, \Gamma \vdash \Theta}{\exists x\Phi, \Gamma \vdash \Theta}$$

shows that $\exists x\Phi, \Gamma \vdash \Theta$ is also provable. □

In conclusion note a number of simple properties to be used implicitly in what follows. The formulations of the properties assume that all explicitly written out sequents are sequents of G.

1. *If* $\dfrac{\Gamma \vdash \Theta(\Lambda \vdash \Delta)}{\Gamma' \vdash \Theta'}$ *is a passage according to one of the rules of inference, then for any formula* Φ (*such that* $\Gamma \vdash \Theta, \Phi$ *and* $\Lambda \vdash \Phi, \Delta$ *are sequents of the calculus* G)

$$\frac{\Gamma \vdash \Phi, \Theta \quad \Lambda \vdash \Phi, \Delta}{\Gamma' \vdash \Phi, \Theta'} \quad \textit{and} \quad \frac{\Gamma, \Phi \vdash \Theta \quad \Lambda, \Phi \vdash \Delta}{\Gamma', \Phi \vdash \Theta'}$$

are passages corresponding to the same rule of inference.

2. *If* $\dfrac{\Gamma \vdash \Theta}{\Gamma' \vdash \Theta'}$ *is a passage according to one of the rules of inference,* Φ *is a formula such that* $\Gamma, \Phi \vdash \Theta$ *is a sequent of* G *and the passage under consideration is a passage according to Rule* 8 *or* 9, *then the corresponding variables* x *and* y *are not free in* Φ. *Hence*

$$\frac{\Gamma \vdash \Phi, \Theta}{\Gamma' \vdash \Phi, \Theta'} \quad \textit{and} \quad \frac{\Gamma, \Phi \vdash \Theta}{\Gamma', \Phi \vdash \Theta'}$$

are passages corresponding to the same rule of inference.

3. *If* $\frac{\Gamma \vdash \Theta(\Lambda \vdash \Delta)}{\Gamma' \vdash \Theta'}$ *is a passage according to one of the rules of inference and* Φ *occurs in* $\Gamma'(\Theta')$, *then the passage*

$$\frac{\Gamma^* \vdash \Theta\ (\Lambda^* \vdash \Delta)}{\Gamma'^* \vdash \Theta'} \qquad \left(\frac{\Gamma \vdash \Theta^*\ (\Lambda \vdash \Delta^*)}{\Gamma' \vdash \Theta'^*}\right)$$

where Γ^*, $\Lambda^*(\Theta^*, \Delta^*)$ *is obtained by eliminating from* Γ, $\Lambda(\Theta, \Delta)$ *the ancestors of the occurrence of* Φ *in* $\Gamma'(\Theta')$ *and* $\Gamma'^*(\Theta'^*)$ *is obtained from* $\Gamma'(\Theta')$ *by eliminating the occurrence of* Φ, *is either a passage according to the same rule of inference or a trivial passage* (*i. e. the sequents above the line coincide with the lower sequent of this passage*).

Exercises

1. Show that for any formula Φ of CP^Σ there is an equivalent formula Ψ satisfying the condition that the variables should be unmixed.
2. Verify that a formula of CP^Σ in prenex normal form satisfies the condition that it should have unmixed variables.
3. Let us extend the language of the calculus G by permitting formulas and sequents also without the condition that they should have unmixed variables. Establish that an identically true sequent $P(x) \vdash \exists y \forall x P(y)$ is not provable in the resulting calculus G^*.

31. THE INVERTIBILITY OF RULES

Most rules of inference of the calculus G possess yet another remarkable property that can be used in searching for a derivation in the calculus. It is the property of invertibility consisting (in somewhat rough terms) in that the sequent below the line in a rule is provable if and only if so are the sequents (so is the sequent) above the line.

We first formulate and prove this property for the propositional rules.

PROPOSITION 1. (1) *If a sequent* $\Gamma \vdash \Theta, \Phi \wedge \Psi$ *is provable, then so are sequents* $\Gamma \vdash \Theta, \Phi$ *and* $\Gamma \vdash \Theta, \Psi$; (2) *if a sequent* $\Phi \wedge \Psi, \Gamma \vdash \Theta$ *is provable, then so is a sequent* $\Phi, \Psi, \Gamma \vdash \Theta$; (3) *if a sequent* $\Gamma \vdash \Theta, \Phi \vee \Psi$ *is provable, then so is a sequent* $\Gamma \vdash \Theta, \Phi, \Psi$; (4) *if a sequent* $\Phi \vee \Psi, \Gamma \vdash \Theta$ *is provable, then so are sequents* Φ,

$\Gamma \vdash \Theta$ *and* $\Psi, \Gamma \vdash \Theta$; (5) *if a sequent* $\Gamma \vdash \Theta, \neg\Phi$ *is provable, then so is a sequent* $\Phi, \Gamma \vdash \Theta$; (6) *if a sequent* $\neg\Phi, \Gamma \vdash \Theta$ *is provable, then so is a sequent* $\Gamma \vdash \Theta, \Phi$.

PROOF. Verification of all the statements of the proposition is tedious and monotonous. Therefore we prove some typical cases, statements (1) and (6), for example. We shall carry out verification by induction on the height of a proof (see also the proof of Lemma 9.2).

Statement (1) will be proved in a slightly more general form and only for a formula Φ: if a sequent $\Gamma \vdash \Theta, \Phi \wedge \Psi, \Lambda$ is provable, then so is a sequent $\Gamma \vdash \Theta, \Phi, \Lambda$, there being a proof of the latter sequent with fewer passages than in the proof of the original sequent.

Let the proof D of the sequent $\Gamma \vdash \Theta, \Phi \wedge \Psi, \Lambda$ be of the form

$$\frac{D_0 \quad D_1}{C}.$$

If $\Phi \wedge \Psi$ is a principal formula of the last passage, then D_0 is a proof of the sequent $\Gamma \vdash \Theta, \Phi, \Lambda$ (in this case Λ is an empty sequence of formulas) and D_0 has fewer passages than D.

If $\Phi \wedge \Psi$ is not the principal formula of the last passage, then the final sequents C_0 and C_1 of the proofs D_0 and D_1 are of the form $\Gamma_0 \vdash \Theta_0, \Phi \wedge \Psi, \Lambda_0$ and $\Gamma_1 \vdash \Theta, \Phi \wedge \Psi, \Lambda_1$ respectively, where the singled out occurrences of $\Phi \wedge \Psi$ in C_0 and C_1 are the ancestors of the given occurrence of the formula $\Phi \wedge \Psi$ in the sequent C. By the induction hypothesis there are proofs D_0' and D_1' of the sequents $\Gamma_0 \vdash \Theta_0, \Phi, \Lambda_0$ and $\Gamma_1 \vdash \Theta_1, \Phi, \Lambda_1$ respectively. Then the tree of sequents

$$\frac{D_0' \qquad D_1'}{\Gamma \vdash \Theta, \Phi, \Lambda}$$

is a proof. (Since $\Phi \wedge \Psi$ was not the principal formula of the passage

$$\frac{\Gamma_0 \vdash \Theta_0, \Phi \wedge \Psi, \Lambda_0 \qquad \Gamma_1 \vdash \Theta_1, \Phi \wedge \Psi, \Lambda_1}{\Gamma \vdash \Theta, \Phi \wedge \Psi, \Lambda},$$

the passage

$$\frac{\Gamma_0 \vdash \Theta_0, \Phi, \Lambda_0 \qquad \Gamma_1 \vdash \Theta_1, \Phi, \Lambda_1}{\Gamma \vdash \Theta, \Phi, \Lambda},$$

is effected according to the same rule as the first passage.)

Let the proof of the sequent C be of the form

$$\frac{D_0}{C}.$$

If the last passage is not effected by Rule 13 applied to $\Phi \wedge \Psi$ and $C_0 = \Gamma_0 \vdash \Theta_0, \Phi \wedge \Psi, \Lambda_0$ is the final sequent of D_0, then by the induction hypothesis there is a proof D_0' of the sequent $\Gamma_0 \vdash \vdash \Theta_0, \Phi, \Lambda_0$ and the tree

$$\frac{D_0'}{\Gamma \vdash \Theta, \Phi, \Lambda}$$

is the proof.

Let the last passage in the tree D be

$$\frac{\Gamma \vdash \Theta, \Phi \wedge \Psi, \Phi \wedge \Psi}{\Gamma \vdash \Theta, \Phi \wedge \Psi}.$$

By the induction hypothesis there is a proof D_0' of the sequent $\Gamma \vdash \Theta, \Phi \wedge \Psi, \Phi$, the number of passages in D_0' being less than that of passages in D_0. Again by the induction hypothesis there is a proof D_0'' of the sequent $\Gamma \vdash \Theta, \Phi, \Phi$. Then

$$\frac{D_0''}{\Gamma \vdash \Theta, \Phi}$$

is the required proof.

We now prove statement (6). Let D be a proof of a sequent $C_0 = \neg\Phi, \Gamma \vdash \Theta$; it may be assumed by Lemma 2 of the preceding section that the proof D possesses the property of the purity of the variables. Let us pass from the tree D to a tree D' by making the following transformations: we replace each occurrence of a sequent $C = \Lambda \vdash \Delta$ by an occurrence of a sequent $C' = \Lambda' \vdash \Phi, \Delta'$, where Λ' and Δ' are obtained from Λ and Δ by eliminating all the ancestors of the formula $\neg\Phi$ of the final occurrence of C_0 which have the form Φ or $\neg\Phi$. (*Remark.* It is easy to verify by induction that an ancestor of the formula $\neg\Phi$ of the form $\neg\Phi$ may be only on the left-hand side of the sequent and that an ancestor of the form Φ may be only on the right-hand side.) We verify that D' is a quasi-derivation of the sequent $\Gamma \vdash \Phi, \Theta$. This is obviously sufficient for the sequent $\Gamma \vdash \Theta, \Phi$ to be provable. If $C = \Lambda \vdash \Delta$

is an axiom, then $\Lambda' = \Lambda$; if the last formula in Δ is an ancestor of $\neg\Phi$ of the form Φ, then $\Lambda' \vdash \Phi, \Delta'$ is obtained from the axiom $\Lambda \vdash \Delta$ by applying only the interchange rules. If the last formula in Δ is not an ancestor of $\neg\Phi$ of the form Φ, then $\Lambda' \vdash \Delta'$ is an axiom and $\Lambda' \vdash \Phi, \Delta'$ is obtained from it by the rule of revision (Lemma 3 of Sec. 30) and by interchanges.

We now look at the passages of the tree D'. It is easily verified that if in a passage of the tree D no ancestor of the formula $\neg\Phi$ of the form Φ or $\neg\Phi$ is the principal formula, then the corresponding passage in D' is effected by the same rule of inference. Now consider cases where an ancestor of $\neg\Phi$ of the form Φ or $\neg\Phi$ is the principal formula of a passage. Then that passage may be effected only by Rules 1, 3, 5, 6, 7, 9 or by the structural rules 11 to 14.

An analysis of every case is not necessary. Let us consider the cases of applying Rules 1, 5, 6, 9, 13.

Let a passage in D be of the form

$$\frac{\Delta \vdash \Lambda, \Psi \quad \Delta \vdash \Lambda, \mathrm{X}}{\Delta \vdash \Lambda, \Psi \wedge \mathrm{X}}$$

and $\Phi = \Psi \wedge \mathrm{X}$ be an ancestor of $\neg\Phi$, then the passage in D' is

$$\frac{\Delta' \vdash \Phi, \Lambda', \Psi \quad \Delta' \vdash \Phi, \Lambda', \mathrm{X}}{\Delta' \vdash \Phi, \Lambda'}$$

and the lower sequent can be obtained from the upper ones by the rules of introducing a conjunction (1), of interchange (11) and of abbreviation (13).

Let a passage in D be of the form

$$\frac{\Psi, \Delta \vdash \Lambda}{\Delta \vdash \Lambda, \neg\Psi}$$

and let $\Phi = \neg\Psi$ be an ancestor of $\neg\Phi$, then the passage in D' is

$$\frac{\Psi, \Delta' \vdash \Lambda'}{\Delta' \vdash \Phi, \Lambda'}$$

but since $\Phi = \neg\Psi$, the lower sequent is obtained from the upper one by applying the rule of introducing a negation (5), by the interchange rule (11) and the abbreviation rule (13).

Let a passage in D be of the form

$$\frac{\Delta \vdash \Lambda, \Phi}{\neg\Phi, \Delta \vdash \Lambda}$$

and let Φ and $\neg\Phi$ be ancestors of the formula $\neg\Phi$ (in the final sequent), then the corresponding passage in D' is

$$\frac{\Delta' \vdash \Phi, \Lambda'}{\Delta' \vdash \Phi, \Lambda'},$$

i. e. is trivial.

Let a passage in D be of the form

$$\frac{\Delta \vdash \Lambda, [\Psi]^x_y}{\Delta \vdash \Lambda, \forall x\Psi}$$

and let $\Phi = \forall x\Psi$ be an ancestor of $\neg\Phi$, then the corresponding passage in D' is

$$\frac{\Delta' \vdash \Phi, \Lambda', [\Psi]^x_y}{\Delta' \vdash \Phi, \Lambda'}$$

and the lower sequent is obtained from the upper one by applying Rules 9 (this application is legitimate since Δ' and Λ' are parts of Δ and Λ and y is different from all free variables of the formula Φ in that it has the property of the purity of variables in D), 11 and 13.

Finally, let a passage in D be

$$\frac{\Delta \vdash \Lambda, \Phi, \Phi}{\Delta \vdash \Lambda, \Phi}$$

and let Φ be an ancestor of $\neg\Phi$, then in D' the corresponding passage

$$\frac{\Delta' \vdash \Phi, \Lambda'}{\Delta' \vdash \Phi, \Lambda'}$$

is trivial. □

Let us now turn to the quantifier rules.

PROPOSITION 2. (1) *If a sequent* $\exists x\Phi, \Gamma \vdash \Theta$ *is provable in G, then for any term t such that* $(\Phi)^x_y, \Gamma \vdash \Theta$ *is a sequent of G that sequent is provable in G*; (2) *if a sequent* $\Gamma \vdash \Theta, \forall x\Phi$ *is provable, then for any term t such that* $\Gamma \vdash \Theta, (\Phi)^x_y$ *is a sequent that sequent is provable in G.*

The proofs of these statements are similar and therefore we shall give only a proof of statement (2).

Let $y_0, \ldots, y_k$ be all free variables of a term t and let D be a proof of a sequent $\Gamma \vdash \Theta, \forall x\Phi$ that possesses the property of the purity of variables and is such that any variable vanishing in that proof is different from the variables $y_0, \ldots, y_k$. Let $[\Phi]^x_{z0}, \ldots, [\Phi]^x_{z_s}$ be all ancestors of the form $[\Phi]^x_y$ of the occurrence of the formula $\forall x\Phi$ in the final sequent. We construct a tree of sequents D' as follows. Each occurrence of a sequent C in D is replaced by an occurrence of a sequent C' obtained from C by replacing all ancestors of the formula $\forall x\Phi$ of the form $\forall x\Phi$ by $(\Phi)^x_t$ and by substituting a term t for all occurrences of the variables $z_0, \ldots, z_s$. It is easily verified that all initial sequents of the tree D' are axioms and that all the passages of D' are either performed by the same rules as those in the corresponding passage of D or are trivial passages. The latter happens when the corresponding passage in D is

$$\frac{\Delta \vdash \Lambda, [\Phi]^x_z}{\Delta \vdash \Lambda, \forall x\Phi}$$

and $\forall x\Phi$ is an ancestor of the formula $\forall x\Phi$ in the final sequent. Thus D' is a quasi-derivation of the sequent $\Gamma \vdash \Theta, (\Phi)^x_t$. □

COROLLARY. Let y have no occurrences in any of the formulas of a sequent $\Gamma \vdash \Theta, \forall x\Phi$; that sequent (the sequent $\exists x\Phi, \Gamma \vdash \Theta$) is provable if and only if so is a sequent $\Gamma \vdash \Theta, [\Phi]^x_y$ (a sequent $[\Phi]^x_y, \Gamma \vdash \Theta$). □

For Rules 7 and 10 there is no good formulation of invertibility (see Exercise 1) although this property is true in some form "distributed throughout a proof" (cf. the proof of theorem on the elimination of section in the next section).

Exercises

1. Prove that there are no terms $t_0, \ldots, t_k$ such that a sequent $\exists xP \vdash (P)^x_{t0}, \ldots, (P)^x_{t_k}$ is provable although the sequent $\exists xP \vdash \exists xP$ is provable.

2. Prove in G the sequent $\exists zP(z) \vdash \exists y\forall xP(y)$.

3. Show that Proposition 2 is not true in the calculus G^* (see Exercise 3 of Sec. 30). (*Hint.* Use Exercise 2 and Exercise 3 of Sec. 30.)

32. COMPARISON OF THE CALCULI CP^{Σ} AND G

In this section we prove that a sequent of CP^{Σ} which is a sequent of G as well (i. e. does not contain the implication sign $\rightarrow$ and the equality sign $\approx$ and satisfies the condition of the purity of the variables) is CP^{Σ}-provable if and only if it is provable in G.

The proof of this statement is based on the following important theorem of the calculus G.

THEOREM 1 (Cut Elimination). *Let* $\Gamma \vdash \Theta, \Phi$ *and* $\Phi, \Lambda \vdash \Delta$ *be provable sequents of* G. *If* $\Gamma, \Lambda \vdash \Delta, \Theta$ *is a sequent of* G, *then it is provable.*

PROOF. We first prove this theorem for an atomic formula by induction on the number of essential passages in a proof of the sequent $\Gamma \vdash \Theta$, understanding by essential passages those that are performed by rules other than the interchange rules 11 and 12. If $\Gamma \vdash \Theta, \Phi$ has a proof without essential passages, then $\Gamma \vdash \Theta, \Phi$ differs from an axiom only in the interchange of formulas. Consider two possible cases.

1. $\Phi \in \Gamma$; then the sequent $\Gamma, \Lambda \vdash \Delta, \Theta$ can be obtained from a (provable) sequent $\Phi, \Lambda \vdash \Delta$ by applying a derived rule of strengthening (Lemma 3 of Sec. 30) and the interchange rules.

2. There is a formula Ψ such that $\Psi \in \Gamma$ and $\Psi \in \Theta$. Then the sequent $\Gamma \in \Theta$ is provable (interchange of an axiom) and the sequent $\Gamma, \Lambda \vdash \Delta, \Theta$ is obtained from it by strengthening and interchanges.

Suppose that for sequents $\Gamma \vdash \Theta, \Phi$ having a proof with less than $n > 0$ essential passages the theorem is true. Let D be a proof of a sequent $\Gamma \vdash \Theta, \Phi$ having n essential passages; it will be assumed that the proof D has the property of the purity of variables.

Let us consider the lowermost essential passage in D. There are two possibilities:

1. The passage has the form

$$\frac{\Gamma_0 \vdash \Theta_0', \Phi, \Theta_0'' \quad \Gamma_1 \vdash \Theta_1', \Phi, \Theta_1''}{\Gamma' \vdash \Theta', \Phi, \Theta''} \qquad (*)$$

Here Γ' is an interchange of Γ; Θ', Θ'' is an interchange of Θ; the indicated occurrences of the formula Φ are ancestors of occurrence of Φ in the final sequent $\Gamma \vdash \Theta, \Phi$. The sequents $\Gamma_0 \vdash \Theta_0', \Theta_0'', \Phi$ and $\Gamma_1 \vdash \Theta_1', \Theta_1'', \Phi$ have a proof with a number of essential passage $< n$ (since they are obtained by interchange from the sequents $\Gamma_0 \vdash \Theta_0', \Phi, \Theta_0''$ and $\Gamma_1 \vdash \Theta_1', \Phi, \Theta_1''$). Therefore sequents $\Gamma_0, \Lambda \vdash \Delta, \Theta_0', \Theta_0''$ and $\Gamma_1, \Lambda \vdash \Delta, \Theta_1', \Theta_1''$ are provable. The tree of sequents

$$\cfrac{\cfrac{\Gamma_0, \Lambda \vdash \Delta, \Theta_0', \Theta_0'' \quad \Gamma_1, \Lambda \vdash \Delta, \Theta_1', \Theta_1''}{\Gamma', \Lambda \vdash \Delta, \Theta', \Theta''}}{\Gamma, \Lambda \vdash \Delta, \Theta}$$

is a quasi-derivation, since the atomic formula Φ is not the principal formula of the passage $(*)$.

2. The passage has the form

$$\frac{\Gamma' \vdash \Theta', \Phi, \Phi}{\Gamma' \vdash \Theta', \Phi};$$

Γ' is an interchange of Γ, Θ' is an interchange of Θ and the indicated occurrences of Φ are ancestors of the occurrence of Φ in the final sequent. If D' is a subtree of the tree D defined by the occurrence in D of a sequent $\Gamma' \vdash \Theta', \Phi, \Phi$, then we let D'' be obtained from D' by eliminating in each sequent all ancestors of the right-hand occurrence of a formula Φ in the final sequent $\Gamma' \vdash$ $\vdash \Theta', \Phi, \Phi$. At the tops of D'' are sequents that differ from axioms only in interchange. The passages are either trivial or correspond to the same rules as in D'. A simple rearrangement of D'' yields a proof of the sequent $\Gamma' \vdash \Theta', \Phi$ (and hence a proof of the sequent $\Gamma \vdash \Theta, \Phi$) with a number of essential passages equal to the number of essential passages in D'. Since there are fewer essential passages in D' than in D, by the induction hypothesis the sequent $\Gamma, \Lambda \vdash \Delta, \Theta$ is provable.

3. The passage has the form

$$\frac{\Gamma_0 \vdash \Theta_0', \Phi, \Theta_0''}{\Gamma' \vdash \Theta', \Phi, \Theta''};$$

Γ' is an interchange of Γ; Θ', Θ'' is an interchange of Θ; the indicated occurrences of Φ are ancestors of Φ in the final sequent of the tree D and Φ is not the principal formula of the passage.

The sequent $\Gamma_0 \vdash \Theta_0', \Theta_0'', \Phi$ is obtained from $\Gamma_0 \vdash \Theta_0', \Phi, \Theta_0''$ by interchange and therefore it has a proof with the number of essential passages $n - 1$. Then by the induction hypothesis the sequent $\Gamma_0, \Lambda \vdash \Delta, \Theta_0', \Theta_0''$ is provable. The tree of sequents

$$\cfrac{\cfrac{\Gamma_0, \Lambda \vdash \Delta, \Theta_0', \Theta_0''}{\Gamma', \Lambda \vdash \Delta, \Theta', \Theta''}}{\Gamma, \Lambda \vdash \Delta, \Theta}$$

is a quasi-derivation.

So for sequents $\Gamma \vdash \Theta, \Phi$ with an atomic formula Φ the theorem is established.

We proceed by induction on the construction of a formula Φ. Assuming that for the proper (i. e. not equal to Φ) generalized subformulas of a formula Φ and any $\Gamma, \Lambda, \Theta, \Delta$ the theorem is true we establish the validity of the theorem for Φ as well.

Let $\Phi = \Psi \wedge X$; $\Gamma \vdash \Theta, \Phi$ and $\Phi, \Lambda \vdash \Delta$ be provable sequents and let $\Gamma, \Lambda \vdash \Delta, \Theta$ be a sequent of G. Also provable, by invertibility (Proposition 1 of Sec. 31), are the sequents $\Gamma \vdash \Theta\Psi$; $\Gamma \vdash \Theta, X$; $\Psi, X, \Lambda \vdash \Delta$. It follows by the induction hypothesis that also provable are the sequents $\Gamma, X, \Lambda \vdash \Delta, \Theta$; $X, \Gamma, \Lambda \vdash \Delta, \Theta$; $\Gamma, \Gamma, \Lambda \vdash \Delta, \Theta, \Theta$ and, finally, the sequent $\Gamma, \Lambda \vdash \Delta, \Theta$.

The cases $\Phi = \Psi \vee X$, $\Phi = \neg \Psi$ are treated similarly.

Now let $\Phi = \forall x \Psi$; $\Gamma \vdash \Theta, \Phi$; $\Phi, \Lambda \vdash \Delta$ be provable sequents and let $\Gamma, \Lambda \vdash \Delta, \Theta$ be a sequent of G. Let D be a proof of the sequent $\Phi, \Lambda \vdash \Delta$. It is assumed that D has the property of the purity of variables and that any variable y vanishing in D is different from all the variables of the formulas in the list Γ, Θ. We establish by induction on the depth of an occurrence in the tree D that for any occurrence of a sequent $\Lambda' \vdash \Delta'$ in D the sequent $\Lambda'^*, \Gamma \vdash \Theta, \Delta'$ is provable, where Λ'^* is obtained from Λ' by eliminating all ancestors of a formula Φ in the final sequent of the form Φ.

It is clear that for the uppermost occurrences ($\Lambda' \vdash \Delta'$ is an axiom) the corresponding sequent ($\Lambda', \Gamma \vdash \Theta, \Delta'$) is provable (is obtained by applications of the rule of strengthening). Let us consider a passage in D

$$\frac{\Lambda_0 \vdash \Delta_0 \qquad \Lambda_1 \vdash \Delta_1}{\Lambda' \vdash \Delta'}$$

and suppose that the sequents $\Lambda_0^*, \Gamma \vdash \Theta, \Delta_0$; $\Lambda_1^*, \Gamma \vdash \Theta, \Delta_1$ corresponding to the upper occurrences are provable. Then

$$\frac{\Lambda_0^*, \Gamma \vdash \Theta, \Delta_0 \qquad \Lambda_1^*, \Gamma \vdash \Theta, \Delta_1}{\Lambda'^*, \Gamma \vdash \Theta, \Delta'}$$

is easily seen to be a passage according to the same rule of inference and hence a quasi-derivation. The situation is similar for one-hypothesis passages, except for passages of the form

$$\frac{(\Psi)_t^x, \quad \Lambda_0 \vdash \Delta_0}{\forall x \Psi, \quad \Lambda_0 \vdash \Delta_0},$$

where the occurrence of $\Phi = \forall x \Psi$ in the lower sequent is an ancestor of the formula Φ of the final sequent of the tree D. Corresponding to the occurrences in that passage there are sequents $(\Psi)_t^x, \Lambda_0^*, \Gamma \vdash \Theta, \Delta_0$ and $\Lambda_0^*, \Gamma \vdash \Theta, \Delta_0$. Suppose that the sequent $(\Psi)_t^x, \Lambda_0^*, \Gamma \vdash \Theta, \Delta_0$ is provable. Under the hypothesis of the theorem the sequent $\Gamma \vdash \Theta, \forall x \Psi$ is a provable sequent and therefore so is the sequent $\Gamma \vdash \Theta, (\Psi)_t^x$ by Proposition 31.2. Since $(\Psi)_t^x$ is a proper generalized subformula of the formula $\Phi = \forall x \Psi$, applying the induction hypothesis on the validity of the theorem for proper generalized subformulas of a formula Φ to the provable sequents $(\Psi)_t^x, \Lambda_0^*, \Gamma \vdash \Theta, \Delta_0$ and $\Gamma \vdash \Theta, (\Psi)_t^x$ we conclude that the sequent $\Gamma, \Lambda_0^*, \Gamma \vdash \Theta, \Delta_0, \Theta$ is provable. Using the rules of interchange and abbreviation we obtain from the provability of the last sequent the provability of the sequent $\Lambda_0^*, \Gamma \vdash \Theta, \Delta_0$.

So for each occurrence of the sequent $\Lambda' \vdash \Delta'$ in D the corresponding sequent $\Lambda'^*, \Gamma \vdash \Theta, \Delta'$ is provable. Corresponding to the final sequent of the tree D there is a provable sequent $\Lambda, \Gamma \vdash \vdash \Theta, \Delta$. From this, using the interchange rule we obtain the provability of the sequent $\Gamma, \Lambda \vdash \Delta, \Theta$.

The case where Φ is of the form $\exists x \Psi$ is treated similarly. □

Remark. It may be assumed that Theorem 1 establishes that the following rule (the cut rule) is admissible

$$\frac{\Gamma \vdash \Theta, \Phi \qquad \Phi, \Lambda \vdash \Delta}{\Gamma, \Lambda \vdash \Delta, \Theta}.$$

We now proceed to prove the main statement. If $\Theta = \Phi_1, \ldots, \Phi_n$ is a list of formulas, then by $\neg \Theta$ we shall denote the list $\neg \Phi_1, \ldots, \neg \Phi_n$.

PROPOSITION 1. *If a sequent* $C = \Gamma \vdash \Theta$ *is provable in* G, *then the sequent* $C' = \Gamma, \neg\Theta \vdash$ *is provable in* CP^{Σ}.

PROOF. By induction on the height of the proof in G. If $\Phi, \Gamma \vdash \vdash \Theta, \Phi$ is an axiom, then the sequent $\Phi, \Gamma, \neg\Theta \vdash \Phi$ is provable in CP^{Σ} using the axiom $\Phi \vdash \Phi$ and the rule of adding an extra hypothesis; finally

$$\dfrac{\Phi, \Gamma, \neg\Theta \vdash \Phi \qquad \neg\Phi \vdash \neg\Phi}{\Phi, \Gamma, \neg\Theta, \neg\Phi \vdash}$$

is a quasi-derivation in CP^{Σ} of the required sequent.

Now it is necessary to verify for each rule of inference that if the sequents C_0 (and C_1) above the line in the rule are such that C_0' (and C_1') are provable in CP^{Σ}, then so is the sequent C' corresponding to the sequent C below the line. Checking all the rules is rather tiresome and therefore we shall check only Rules 2, 3, 5, 7, 8, 10.

(2) Let a sequent $\Phi, \Psi, \Gamma, \neg\Theta \vdash$ be provable in CP^{Σ}. Then the following tree of sequents is a quasi-derivation in CP^{Σ}:

$$\dfrac{\dfrac{\Phi \wedge \Psi \vdash \Phi \wedge \Psi}{\Phi \wedge \Psi \vdash \Psi} \qquad \dfrac{\dfrac{\dfrac{\Phi \wedge \Psi \vdash \Phi \wedge \Phi}{\Phi \wedge \Psi \vdash \Phi} \quad \dfrac{\Phi, \Psi, \Gamma, \neg\Theta \vdash}{\Psi, \Gamma, \neg\Theta \vdash \neg\Phi}}{\Phi \wedge \Psi, \Psi, \Gamma, \neg\Theta \vdash}}{\Phi \wedge \Psi, \Gamma, \neg\Theta \vdash \neg\Psi}}{\Phi \wedge \Psi, \Gamma, \neg\Theta \vdash .}$$

(3) Let a sequent $\Gamma, \neg\Theta, \neg\Phi, \neg\Psi \vdash$ be provable in CP^{Σ}. Then the following tree of sequents is a quasi-derivation in CP^{Σ}:

$$\dfrac{\dfrac{\vdash \Phi \vee \neg\Phi \quad \dfrac{\Phi \vdash \Phi}{\Phi \vdash \Phi \vee \Psi} \quad \dfrac{\dfrac{\Gamma, \neg\Theta, \neg\Phi, \neg\Psi \vdash}{\Gamma, \neg\Theta, \neg\Phi \vdash \Psi}}{\Gamma, \neg\Theta, \neg\Phi \vdash \Phi \vee \Psi}}{\Gamma, \neg\Theta \vdash \Phi \vee \Psi} \qquad \neg(\Phi \vee \Psi) \vdash \neg(\Phi \vee \Psi)}{\Gamma, \neg\Theta, \neg(\Phi \vee \Psi) \vdash}\,.$$

(5) Let a sequent $\Phi, \Gamma, \neg\Theta \vdash$ be provable in CP^{Σ}. Then

$$\dfrac{\dfrac{\Phi, \Gamma, \neg\Theta \vdash}{\Gamma, \neg\Theta \vdash \neg\Phi} \qquad \neg\neg\Phi \vdash \neg\neg\Phi}{\Gamma, \neg\Theta, \neg\neg\Phi \vdash}$$

is a quasi-derivation in CP^{Σ}.

(7) Let a sequent $\Gamma, \neg\Theta, \neg(\Phi)^x_t \vdash$ be provable in CP^{Σ}. Then

$$\dfrac{\dfrac{\dfrac{\Gamma, \neg\Theta, \neg(\Phi)^x_t \vdash}{\Gamma, \neg\Theta \vdash (\Phi)^x_t}}{\Gamma, \neg\Theta \vdash \exists x\Phi} \qquad \neg\exists x\Phi \vdash \neg\exists x\Phi}{\Gamma, \neg\Theta, \neg\exists x\Phi \vdash}$$

is a quasi-derivation in CP^{Σ}.

(8) Let a sequent $[\Phi]^x_y, \Gamma, \neg\Theta \vdash$ be provable in CP^{Σ} and let y have no free occurrences in $\Gamma, \neg\Theta$. Then

$$\dfrac{\exists x\Phi \vdash \exists y[\Phi]^x_y \qquad \dfrac{\dfrac{[\Phi]^x_y, \Gamma, \neg\Theta \vdash}{\exists y[\Phi]^x_y, \Gamma, \neg\Theta \vdash}}{\Gamma, \neg\Theta \vdash \neg\exists y[\Phi]^x_y}}{\exists x\Phi, \Gamma, \neg\Theta \vdash}$$

is a quasi-derivation in CP^{Σ}.

(10) Let a sequent $(\Phi)^x_t, \Gamma, \neg\Theta \vdash$ be provable in CP^{Σ}. Then

$$\dfrac{(\Phi)^x_t, \Gamma, \neg\Theta \vdash}{\forall x\Phi, \Gamma, \neg\Theta \vdash}$$

is a quasi-derivation in CP^{Σ}.

Verification of the remaining rules is quite similar. Induction on the height of a proof in G completes the proof of the proposition. □

PROPOSITION 2. *If a sequent C of G is provable in* CP^{Σ}, *then it is provable in G too.*

PROOF. We first establish the provability in G of axioms $\Phi \vdash \Phi$ of CP^{Σ} by induction on the construction of a formula Φ. If Φ is an atomic formula, then $\Phi \vdash \Phi$ is an axiom of G. Let sequents $\Phi \vdash \Phi$ and $\Psi \vdash \Psi$ be provable in G for formulas Φ and Ψ. Consider the following quasi-derivations in G:

$$\dfrac{\dfrac{\dfrac{\Phi \vdash \Phi}{\Phi, \Psi \vdash \Phi}}{\Phi \wedge \Psi \vdash \Phi} \qquad \dfrac{\dfrac{\Psi \vdash \Psi}{\Phi, \Psi \vdash \Psi}}{\Phi \wedge \Psi \vdash \Psi}}{\Phi \wedge \Psi \vdash \Phi \vee \Psi} \qquad \dfrac{\dfrac{\dfrac{\Phi \vdash \Phi}{\Phi \vdash \Phi, \Psi}}{\Phi \vdash \Phi \vee \Psi} \qquad \dfrac{\dfrac{\Psi \vdash \Psi}{\Psi \vdash \Phi, \Psi}}{\Psi \vdash \Phi \vee \Psi}}{\Phi \vee \Psi \vdash \Phi \vee \Psi}$$

$$\dfrac{\dfrac{\dfrac{\Phi \vdash \Phi}{\vdash \Phi, \neg\Phi}}{\vdash \neg\Phi, \Phi}}{\neg\Phi \vdash \neg\Phi} \qquad \dfrac{\dfrac{[\Phi]^x_y \vdash [\Phi]^x_y}{[\Phi]^x_y \vdash \exists x\Phi}}{\exists x\Phi \vdash \exists x\Phi} \qquad \dfrac{\dfrac{[\Phi]^x_y \vdash [\Phi]^x_y}{\forall x\Phi \vdash [\Phi]^x_y}}{\forall x\Phi \vdash \forall x\Phi}.$$

In the last two quasi-derivations the variable y is chosen to have no occurrences in Φ. These quasi-derivations show that it is possible to complete the inductive proof of the fact that all sequents of the form $\Phi \vdash \Phi$, with Φ a formula of G, are provable in G.

Now it is necessary to verify for each rule of inference of CP^{Σ} (except for the rules concerning implication) that if the sequents above the line are provable in G, then the sequent below the line is also provable in G. Rules 1, 11, 13 to 16 of CP^{Σ} are instances of the rules of inference of G. For Rules 2 and 3

$$\frac{\Gamma \vdash \Phi \wedge \Psi}{\Gamma \vdash \Phi} \qquad \frac{\Gamma \vdash \Phi \wedge \Psi}{\Gamma \vdash \Psi}.$$

the required statement follows from the corresponding property of invertibility (Proposition 31.2). For Rule 4 (5)

$$\frac{\Gamma \vdash \Phi}{\Gamma \vdash \Phi \vee \Psi} \qquad \left(\frac{\Gamma \vdash \Psi}{\Gamma \vdash \Phi \vee \Psi}\right)$$

a quasi-derivation in G

$$\begin{array}{c} \Gamma \vdash \Phi \\ \hline \Gamma \vdash \Phi, \Psi \\ \hline \Gamma \vdash \Phi \vee \Psi \end{array} \qquad \left(\begin{array}{c} \Gamma \vdash \Psi \\ \hline \Gamma \vdash \Psi, \Phi \\ \hline \Gamma \vdash \Phi, \Psi \\ \hline \Gamma \vdash \Phi \vee \Psi \end{array}\right)$$

establishes the required property. We now consider Rule 6

$$\frac{\Gamma \vdash \Phi \vee \Psi \quad \Gamma, \Phi \vdash X \quad \Gamma, \Psi \vdash X}{\Gamma \vdash X}.$$

If the sequents above the line are provable in G, then the following tree which makes use of the admissible cut rule (see the remark following the proof of Theorem 1) is a quasi-derivation in G

$$\dfrac{\dfrac{\Gamma \vdash \Phi \vee \Psi \qquad \dfrac{\dfrac{\Gamma, \Phi \vdash X}{\Phi, \Gamma \vdash X} \quad \dfrac{\Gamma, \Psi \vdash X}{\Psi, \Gamma \vdash X}}{\Phi \vee \Psi, \Gamma \vdash X}}{\Gamma, \Gamma \vdash X}}{\Gamma \vdash X}$$

Corresponding to Rule 9 there is the statement about the invertibility of the rule of introducing a negation.

For Rule 10, if $\Gamma \vdash \Phi$ and $\Gamma \vdash \neg\Phi$ are provable in G, then so is (by invertibility) the sequent $\Phi, \Gamma \vdash$ and (by Theorem 1) the sequent $\Gamma, \Gamma \vdash$ and hence the sequent $\Gamma \vdash$. The admissibility of Rule 12 in G has been established earlier.

Induction on the height of a proof of the sequent C in CP^{Σ} completes the proof. □

A consequence of Propositions 1 and 2 is the main statement of this section.

THEOREM 2. *A sequent of* CP^{Σ} *which is a sequent of G is provable in* CP^{Σ} *if and only if it is provable in G.* □

Exercise

1. Show that Theorem 1 is not true in the calculus G^* (see Exercise 3 of Sec. 30). (*Hint.* Use the results of Exercise 2 of Sec. 31 and Exercise 3 of Sec. 30.)

33. HERBRAND THEOREM

In this section we shall establish a very important theorem of Herbrand which is, in particular, a theoretical basis of modern machine methods of searching for a proof in the calculus of predicates. One of such methods is based on the calculus of resolvents which is to be discussed in the next section. Herbrand's theorem justifies finding by this method the provability of any provable formula of CP; the latter property is called the completeness of the method. In addition this theorem gives certain constructive meaning to arbitrary sentences of the calculus of predicates.

We begin this section by studying some syntactical relations.

We associate with every term t and every variable x some set $F_x(t)$ of function symbols:

(a) if x does not occur in t or $t = x$, then $F_x(t) = \varnothing$;

(b) if x occurs in t and $t \neq x$, then $t = h(t_1, \ldots, t_n)$ for some function symbol h and some terms $t_1, \ldots, t_n$; we then set $F_x(t) =$

$$= \{h\} \cup \bigcup_{i=1}^{n} F_x(t_i).$$

LEMMA 1. *If $x \neq y$ and x does not occur in t', then for any term t*

$$F_x((t)^y_{t'}) = F_x(t).$$

PROOF. By induction on the construction of a term t. □

PROPOSITION 1. *If $Qx\Psi$ ($Q \in \{\forall, \exists\}$) is a generalized subformula of a formula Φ, then for any term t_0 of a formula Ψ we can find a term t_1 of Φ such that*

$$F_x(t_0) = F_x(t_1)$$

and t_1 is within the scope of the quantifier Qx.

PROOF. Since $Qx\Psi$ is a generalized subformula of a formula Φ, there is a sequence of formulas $\Phi_0 = \Phi, \Phi_1, \ldots, \Phi_n = Qx\Psi$ such that for any $i < n$ one of the following conditions holds:

(1) $\Phi_i = \neg\Phi_{i+1}$;

(2) $\Phi_i = \Phi_{i+1}\tau\Psi_{i+1}$ ($\Phi_i = \Psi_{i+1}\tau\Phi_{i+1}$) for a suitable formula Ψ_{i+1} and $\tau \in \{\vee, \wedge\}$;

(3) $\Phi_i = Q'_y X_i$, $\Phi_{i+1} = (X_i)^y_t$ for a suitable formula X_i and a suitable term t free for a variable y in X_i and $Q' \in \{\forall, \exists\}$.

We now suppose that this proposition is true for $n - 1$. If we take as Φ the formula Φ_1 of the sequence $\Phi = \Phi_0, \Phi_1, \ldots, \Phi_n = Q_x\Psi$, then by the induction hypothesis we can find for any term t_0 of the formula Ψ a term t_2 in Φ_1 such that $F_x(t_0) = F_x(t_1)$ and t_1 is within the scope of the quantifier Qx. If the passage from Φ_0 to Φ_1 satisfies condition (1) or (2), then Φ_1 is a subformula (and not only a generalized subformula) of a formula $\Phi = \Phi_0$, and therefore we must take as the desired t_1 the corresponding term t_2. If condition (3) holds, then we consider three possible subcases.

Subcase (3a): $y = x$. Then $\Phi = Q'xX$, $\Phi_1 = (X)^x_t$ for a suitable formula X. Since Φ_1 (and hence X) has (by the induction hypothesis) free occurrences of the variable x, by the property of the purity of variables x does not occur free in X and $\Phi_1 = X$, $\Phi = Q'_x\Phi_1$; Φ_1 is a subformula of Φ.

Subcase (3b): $y \neq x$ and x occurs in t. Then $\Phi = Q'_y X$, $\Phi_1 = (X)^y_t$ for some formula X. The formula Φ_1 has bound occurrences of the variable x; if X had free occurrences of y, then this would violate the condition that the term t should be free for the variable y in X. So y has no free occurrences in X and $\Phi_1 = (X)^y_t = X$; $\Phi = Q'_y\Phi_1$; Φ_1 is a subformula of Φ.

Subcase (3c): $y \neq x$ and x does not occur in t. Let X be a formula such that $\Phi_1 = (\mathrm{X})^y_t$, $\Phi = Q'_y\,\mathrm{X}$. For any term t_2 of Φ_1 there is a corresponding term t_1 of X such that $t_2 = (t_1)^y_t$, and if t_2 is within the scope of some quantifier in Φ_1, then t_1 is within the scope of the same quantifier for the same variable. By Lemma 1 we have $F_x(t_2) = F_x((t_1)^y_t = F_x(t_1)$; if a term t_2 is chosen in Φ_1 for t_0 in accordance with the conclusion of the proposition, then the corresponding term t_1 will satisfy the conclusion of the proposition for the formula Φ.

The proposition is thus proved. □

We shall say that a function symbol g has a bound occurrence in a formula Φ if Φ contains a subformula of the form $Qx\Psi$ and Ψ has an occurrence of a term t such that $g \in F_x(t)$.

We give two corollaries of Proposition 1.

COROLLARY 1. *If Ψ is a generalized subformula of a formula Φ and a function symbol g occurs bound in Ψ, then g occurs bound in Φ as well.* □

COROLLARY 2. *If D is a proof of a sequent C in G and a function symbol g does not occur bound in any of the formulas C, then g does not occur bound in any of the formulas of the tree D.*

PROOF. By the property of being a subformula and Corollary 1. □

We fix a term t_0, which begins with a function symbol g, and a variable x_0. Now we define a transformation s (heavily relying on the choice of a pair $\langle t_0, x_0\rangle$) of terms as follows:

(a) if t is a variable or a constant (distinct from g), then $s(t) = t$;

(b) if $t = f(t_1, \ldots, t_n)$ and $t \neq t_0$, then $s(t) = f(s(t_1), \ldots, s(t_n))$;

(c) if $t = t_0$, then $s(t) = x_0$.

REMARK. If a term t has no occurrences of t_0, then $s(t) = t$.

The following lemma shows mutual relations of a transformation s and a substitution.

LEMMA 2. *If $x \neq x_0$ and $g \notin F_x(t)$, then for any term t'*

$$s((t)^x_{t'}) = (s(t))^x_{s(t')}.$$

PROOF. We shall prove this equation by induction on the construction of the term t. If x does not occur in t, then neither does x occur in $s(t)$ and therefore $s((t)^x_{t'}) = s(t) = (s(t))^x_{s(t')}$. Let x occur in t. Then $t \neq t_0$, since if $t = t_0 = g(t_1, \dots, t_k)$, then $g \in F_x(t)$. If $t = x$, then $s((x)^x_{t'}) = s(t') = (x)^x_{s(t')}$. If $t = h(t_1, \dots, t_n)$, then $(t)^x_{t'} = h((t_1)^x_{t'}, \dots, (t_n)^x_{t'})$ and $s((t)^x_{t'}) = s(h((t_1)^x_{t'}, \dots, (t_n)^x_{t'})) = $ $= h(s((t_1)^x_{t'}, \dots, s((t_n)^x_{t'})$ since $h \in F_x(t)$, $g \notin F_x(t)$ and hence $h((t_1)^x_{t'}, \dots, (t_n)^x_{t'}) \neq t_0$. By the induction hypothesis $h(s((t_1)^x_{t'}, \dots$ $\dots, s((t_n)^x_{t'}) = h((s(t_1)^x_{s(t')}, \dots, (s(t_n))^x_{s(t')}) = (s(t))^x_{s(t')}$. ☐

REMARK. Under the hypotheses of the lemma $s(t) = t$ according to the remark following the definition of a transformation s.

A transformation of terms s can be extended in a natural way to formulas, sequents and trees of sequents by setting, for example for formulas,

(a) $s(\Phi) = P(s(t_1), \dots, s(t_n))$ for an atomic formula $\Phi = $ $= P(t_1, \dots, t_n)$;

(b) $s(\Phi) = \neg s(\Psi)$ for $\Phi = \neg \Psi$;

(c) $s(\Phi) = s(\Phi_0) \tau s(\Phi_1)$ for $\Phi = \Phi_0 \tau \Phi_1$, $\tau \in \{\vee, \wedge\}$;

(d) $s(\Phi) = Qxs(\Psi)$ for $\Phi = Qx\Psi$, $Q \in \{\forall, \exists\}$.

A consequence of the preceding lemma is

PROPOSITION 2. *If a variable x_0 does not occur bound in Φ and $x \neq x_0$ is a variable such that $g \notin F_x(t)$ for any term t of Φ, then for any term t' free for x in Φ*

$$s((\Phi)^x_{t'}) = (s(\Phi))^x_{s(t')}$$

(this relation also includes the statement that $s(t')$ is free for x in $s(\Phi)$). ☐

Obviously we have also the following

PROPOSITION 2′. *If a variable x_0 does not occur bound in Φ and $x_1, \dots, x_n$ are variables distinct from x_0 and such that $g \notin F_{x_i}(t)$, $i = 1, \dots, n$ for any term t of Φ, then for any terms $t'_1, \dots, t'_n$ free for $x_1, \dots, x_n$ in Φ respectively*

$$s((\Phi)^{x_1, \dots, x_n}_{t'_1, \dots, t'_n}) = (s(\Phi))^{x_1, \dots, x_n}_{s(t'_1), \dots, s(t'_n)}. \qquad \square$$

We establish the following important property of a transformation s operating on proofs.

PROPOSITION 3. *If D is a proof in G, a variable x_0 does not appear in D and g does not occur bound in the final sequent of D, then the tree $s(D)$ is a proof in G.*

PROOF. If $C = \Phi, \Gamma \vdash \Theta, \Phi$ is an axiom, then $s(C) = s(\Phi)$, $s(\Gamma) \vdash s(\Theta)$, $s(\Phi)$ is also an axiom.

For every passage corresponding to a propositional or structural rule, it is easily verified that the corresponding s-passage (i. e. the passage in $s(D)$) is performed according to the same rule of inference. For example, let a passage in D be as follows

$$\frac{\Gamma \vdash \Theta, \Phi \quad \Gamma \vdash \Theta, \Psi}{\Gamma \vdash \Theta, \Phi \wedge \Psi},$$

then the corresponding passage in $s(D)$ is

$$\frac{s(\Gamma) \vdash s(\Theta), s(\Phi) \qquad s(\Gamma) \vdash s(\Theta), s(\Psi)}{s(\Gamma) \vdash s(\Theta), s(\Phi \wedge \Psi)}.$$

But $s(\Phi \wedge \Psi) = s(\Phi) \wedge s(\Psi)$. Hence this passage is effected according to the same rule (introduction of a conjunction into the conclusion).

Now consider passages corresponding to the quantifier rules. Let a passage in D be as follows:

$$\frac{\Gamma \vdash \Theta, (\Phi)_t^x}{\Gamma \vdash \Theta, \exists x \Phi}.$$

Then the corresponding passage in $s(D)$ is

$$\frac{s(\Gamma) \vdash s(\Theta), s((\Phi)_t^x)}{s(\Gamma) \vdash s(\Theta), s(\exists x \Phi)}.$$

According to Corollary 2 of Proposition 1 g does not occur bound in the formula $\exists x \Phi$; hence for any term t' of Φ we have $g \notin$ $\notin F_x(t')$. By Proposition 2 therefore $s((\Phi)_t^x) = (s(\Phi))_{s(t)}^x$. So the passage in the tree $s(D)$ is

$$\frac{s(\Gamma) \vdash s(\Theta), (s(\Phi))_{s(t)}^x}{s(\Gamma) \vdash s(\Theta), \exists x s(\Phi)},$$

but this is a passage effected according to the rule of introducing an existential quantifier into the conclusion.

Now consider a passage in D according to Rule 8:

$$\frac{[\Phi]_y^x, \Gamma \vdash \Theta}{\exists x \Phi, \Gamma \vdash \Theta},$$

where y does not occur free in Γ, Θ. The corresponding passage in $s(D)$ is

$$\frac{s([\Phi]_y^x), s(\Gamma) \vdash s(\Theta)}{s(\exists x \Phi), s(\Gamma) \vdash s(\Theta)}.$$

It is established as before that $s([\Phi]^x_y) = (s(\Phi))^x_{s(y)} = (s(\Phi))^x_y = [s(\Phi)]^x_y$ and that no variable y occurs free in $s(\Gamma)$, $s(\Theta)$. The last statement follows from the fact that for any formula Φ a formula $s(\Phi)$ may contain only one new free variable, namely x_0, which does not appear in D, in particular $x_0 \neq y$. The passage in $s(D)$ is then of the form

$$\frac{[s(\Phi)]^x_y,\, s(\Gamma) \vdash s(\Theta)}{\exists x s(\Phi),\, s(\Gamma) \vdash s(\Theta)},$$

where y does not occur free in $s(\Gamma)$, $s(\Theta)$. Hence this is a passage effected according to Rule 8.

Similarly treated are Rules 9 and 10. □

We now proceed to consider the main statement of this section. For brevity a sequence of terms $t_1, \ldots, t_n$ will be denoted by $\bar{t}$, $\exists \bar{x}$ will denote $\exists x_1 \ldots \exists x_n$; $\bar{z}$ is a sequence $z_1, \ldots, z_k$.

THEOREM 3. *Let a sequent* $C = \Gamma \vdash \Theta, \Phi$ *be such that* $\Phi = \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z})$ *and no n-place function symbol g occurs in C. The sequent C is provable in G if and only if so is a sequent* $C^* = \Gamma \vdash \Theta, \exists \bar{x} \Psi(\bar{x}, g(\bar{x}), \bar{z})$.

Necessity. A *marked formula* is any formula Φ_0 of G of the form

$$(\exists x_{s+1} \ldots \exists x_n \forall y \Psi(\bar{x}, y, \bar{z}))^{x_1, \ldots, x_s}_{t_1, \ldots, t_s},\ 0 \leqslant s \leqslant n,$$

which is a generalized subformula of a formula Φ. If Φ_0 is a marked formula, then Φ_0^* denotes a formula

$$(\exists x_{s+1} \ldots \exists x_n \Psi(\bar{x}, g(\bar{x}), \bar{z}))^{x_1, \ldots, x_s}_{t_1, \ldots, t_s}.$$

Let D be a proof of the sequent C with the property of the purity of variables. Let a tree of sequents D^* be obtained by replacing each occurrence of each marked formula Φ_0 which is an ancestor of the occurrence of Φ in the final sequent C by a formula Φ_0^*. Notice that the final sequent of the tree D^* is C^*. We show that D^* is a quasi-derivation.

At the tops of D^* are the same axioms as in D, since marked formulas are not atomic (contain a quantifier $\forall y$). All passsages in D have corresponding passages in D^* performed according to the same rules of inference, except for passages of the form

$$\frac{\Lambda \vdash \Delta,\ \left[(\Psi(\bar{x}, y, \bar{z}))^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}\right]^{y}_{u}}{\Lambda \vdash \Delta,\ (\forall y \Psi(\bar{x}, y, \bar{z}))^{\bar{x}}_{\bar{t}}}, \tag{$*$}$$

where the principal formula of the passage is a marked formula and ancestor of the formula Φ.

The corresponding passage in D^* is

$$\frac{\Lambda' \vdash \Delta',\ \left[(\Psi(\bar{x}, y, \bar{z}))^{\bar{x}}_{\bar{t}}\right]^{y}_{u}}{\Lambda' \vdash \Delta',\ (\Psi(\bar{x}, g(\bar{x}), \bar{z}))^{\bar{x}}_{\bar{t}}}. \tag{$**$}$$

We use induction on the depth of a derivation and suppose that the sequent above the line in the passage $(**)$ is provable. Since u does not occur in Λ, Δ and Λ', Δ' have the same variables as Λ, Δ, u does not occur in Λ', Δ'; hence the sequent $\Lambda' \vdash \Delta'$, $\forall y(\Psi(\bar{x}, y, \bar{z}))^{\bar{x}}_{\bar{t}}$ is provable. Then so is (by Proposition 2 of Sec. 31) the sequent

$$\Lambda' \vdash \Delta',\ ((\Psi(\bar{x}, y, \bar{z}))^{\bar{x}}_{\bar{t}})^{y}_{g(\bar{t})},$$

but $((\Psi(\bar{x}, y, \bar{z}))^{\bar{x}}_{\bar{t}})^{y}_{g(\bar{t})} = (\Psi(\bar{x}, g(\bar{x}), \bar{z}))^{\bar{x}}_{\bar{t}}$ and therefore the sequent below the line in the passage $(**)$ is provable.

Necessity is thus established.

SUFFICIENCY. A *marked* formula is any formula of the form

$$(\exists x_{s+1} \ldots \exists x_n \Psi(\bar{x}, g(\bar{x}), \bar{z}))^{x_1, \ldots, x_s}_{t_1, \ldots, t_s},\ 0 \leqslant s \leqslant n.$$

Let D be a proof of the sequent C^*. We construct a tree of sequents D^* by replacing each occurrence of a sequent $C' = \Gamma' \vdash \Theta'$ by a sequent $C^+ = \Gamma' \vdash \Theta^+$, where the list of formulas Θ^+ is defined as follows. Let Θ_0 be a list of all formulas of Θ' not simultaneously marked formulas and ancestors of a formula $\exists \bar{x} \Psi(\bar{x}, g(\bar{x}), \bar{z})$ in the final sequent C^*. Let $\bar{t}^1, \ldots, \bar{t}^l$, $l \geqslant 0$, be all n-collections of terms such that the terms $g(\bar{t}^i)$ do not occur in C'; then we set $\Theta_1 = \Phi(= \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z}))$, $\Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots, \Psi(\bar{t}^l, g(\bar{t}^l), \bar{z})$ and $\Theta^+ = \Theta_0, \Theta_1$.

We establish by induction on the depth of a derivation that all sequents of the tree D^* are provable (notice that the final sequent of D^* is the sequent C).

At the tops of D^* are the sequents that can be obtained from the axioms by strengthenings and interchanges.

If a passage is performed in D by one of the Rules 1 to 6, then the corresponding passage in D^* can be obtained by several strengthenings, interchanges and by applying the same rule. This is an easy consequence of the fact that a marked formula which is an ancestor of the formula $\exists \bar{x} \Psi(\bar{x}, g(\bar{x}), \bar{z})$ of the final sequent may be the principal formula of the passage according to one of the Rules 1 to 6 only if $s = n$ and then that formula must necessarily be in the list Θ_1.

If a passage in D is performed according to a structural rule (11 to 14), then the corresponding passage in D^* is obtained by applying structural rules as well.

Consider the case where a passage is performed in D according to Rule 8:

$$\frac{[\Phi_0]^u_v, \Gamma_0 \vdash \Theta_0, \Psi_1, \ldots, \Psi_k}{\exists u \Phi_0, \Gamma_0 \vdash \Theta_0, \Psi_1, \ldots, \Psi_k}, \qquad (*)$$

where $\Psi_1, \ldots, \Psi_k$ is a list of all marked formulas of these sequents that are ancestors of the formula $\exists \bar{x} \Psi(\bar{x}, g(\bar{x}), \bar{z})$ of the final sequent C^*.

The passage in D^* is then

$$\frac{[\Phi_0]^u_v, \Gamma_0 \vdash \Theta_0, \Phi, \Psi, (\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots, \Psi(\bar{t}^m, g(\bar{t}^m), \bar{z})}{\exists u \Phi_0, \Gamma_0 \vdash \Theta_0, \Phi, \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots, \Psi(\bar{t}^l, g(\bar{t}^l), \bar{z})}, \quad l \leqslant m \qquad (**)$$

We show that a variable v does not occur in any of the terms $g(\bar{t}^i)$, $i = 1, \ldots, m$. Suppose the contrary. Let v occur in $g(\bar{t}^i)$; then $g(\bar{t}^i)$ must occur in one of the formulas of the sequent $[\Phi_0]^u_v$, $\Gamma_0 \vdash \Theta_0, \Psi_1, \ldots, \Psi_k$. If $g(\bar{t}^i)$ occurs in one of the formulas of a sequent $\Gamma_0 \vdash \Theta_0, \Psi_1, \ldots, \Psi_k$, then v occurs free in that sequent since otherwise g would occur bound in D, which contradicts Corollary 2 of Proposition 1. But then the passage $(*)$ according to Rule 8 is impossible. If, on the other hand, $g(\bar{t}^i)$ occurs in $[\Phi_0]^u_v$, then the formula $\exists u \Phi_0$ has a bound occurrence of a symbol g, which is impossible. Hence v does not occur free in the sequent $\Gamma_0 \vdash \Theta_0, \Phi, \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots, \Psi(\bar{t}^m, g(\bar{t}^m), \bar{z})$; in addition the sequents $[\Phi_0]^u_v, \Gamma_0 \vdash \Theta_0, \Psi_1, \ldots, \Psi_k$ and $\exists u \Phi_0, \Gamma_0 \vdash \Theta_0, \Psi_1, \ldots, \Psi_k$ have the same occurrences of terms of the form $g(\bar{t})$. But then $l = m$ and the passage $(**)$ is performed according to Rule 8.

Similarly treated is the case of a passage according to Rule 9.

Now consider the case of a passage according to Rule 7. Suppose D has a passage

$$\frac{\Gamma_0 \vdash \Theta_0, \Psi_1, \ldots, \Psi_k, (\Phi_0)^x_t}{\Gamma_0 \vdash \Theta_0, \Psi_1, \ldots, \Psi_k, \exists x \Phi_0}, \qquad (*)$$

where $\Psi_1, \ldots, \Psi_k$ are marked formulas that are ancestors of the formula $\exists \bar{x} \Psi(\bar{x}, g(\bar{x}), \bar{z})$ of the final sequent and the list Θ_0 contains no such formulas.

Two cases are possible: (1) $\exists x \Phi_0$ is neither a marked formula nor an ancestor of the formula $\exists \bar{x} \Psi(\bar{x}), g(\bar{x}), \bar{z})$; (2) it is. Consider case (1). Any term of the form $g(\bar{t})$ in the lower sequent of the passage $(*)$ is simultaneously a term of the upper sequent. Therefore the corresponding passage in D^* is

$$\frac{\Gamma_0 \vdash \Theta_0, (\Phi_0)^x_t, \Phi, \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots, \Psi(\bar{t}^m, g(\bar{t}^m), \bar{z})}{\Gamma_0 \vdash \Theta_0, \exists x \Phi_0, \Phi, \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots, \Psi(\bar{t}^l, g(\bar{t}^l), \bar{z})} \; l \leqslant m. \qquad (**)$$

Let us consider the following tree of sequents instead of $(**)$:

$$\cfrac{\cfrac{\Gamma_0 \vdash \Theta_0, (\Phi_0)^x_t, \Phi, \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots, \Psi(\bar{t}^m, g(\bar{t}^m), \bar{z})}{\Gamma_0 \vdash \Theta_0, \exists x \Phi_0, \Phi, \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots, \Psi(\bar{t}^m, g(\bar{t}^m), \bar{z})}}{\Gamma_0 \vdash \Theta_0, \exists x \Phi_0, \Phi, \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots, \Psi(\bar{t}^l, g(\bar{t}^l), \bar{z})} \, .$$

In this tree the upper passage corresponds (up to an interchange) to an application of Rule 7. Before considering the lower passage we prove the following lemma.

LEMMA 3. *If a sequent*

$$\Gamma \vdash \Theta, \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z}), \Psi(\bar{t}, g(\bar{t}), \bar{z})$$

is provable in G, *the symbol* g *does not occur bound in that sequent and* $g(\bar{t})$ *does not occur in* $\Gamma \vdash \Theta, \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z})$, *then provable in* G *is a sequent*

$$\Gamma \vdash \Theta, \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z}).$$

PROOF. Let D be a proof of the sequent $\Gamma \vdash \Theta, \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z}), \Psi(\bar{t}, g(\bar{t}), \bar{z})$; let x_0 be a variable not appearing in D. If s is a syntactical transformation defined by a pair $\langle x_0, g(\bar{t})\rangle$, then by Proposition 3 the tree $s(D)$ is a proof (of the sequent $\Gamma \vdash \Theta, \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z}), \Psi(\bar{t}, x_0, \bar{z})$ by Proposition 2). Hence the sequent

$\Gamma \vdash \Theta, \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}), (\Psi(\bar{x}, x_0, \bar{z})^{\bar{x}}_{\bar{t}}$ is provable. It is easy to verify that the following tree of sequents

$$\begin{array}{c}
\Gamma \vdash \Theta, \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}), [(\Psi(\bar{x}, y, \bar{z}))^{\bar{x}}_{\bar{t}}]^{y}_{x_0} \\ \hline
\Gamma \vdash \Theta, \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}), (\forall y\Psi(\bar{x}, y, \bar{z})^{x_1, \ldots, x_n}_{t_1, \ldots, t_n} \\ \hline
\Gamma \vdash \Theta, \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}), (\exists x_n\forall y\Psi(\bar{x}, y, \bar{z}))^{x_1, \ldots, x_{n-1}}_{t_1, \ldots, t_{n-1}} \\ \hline
\vdots \\ \hline
\Gamma \vdash \Theta, \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}), \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}) \\ \hline
\Gamma \vdash \Theta, \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z})
\end{array}$$

is a quasi-derivation. □

COROLLARY. *If a sequent* $\Gamma \vdash \Theta, \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}), \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \Psi(\bar{t}^l, g(\bar{t}^l), \bar{z})$ *is provable in G, the symbol g does not occur bound in that sequent and* $g(\bar{t}^i)$ *does not occur in* $\Gamma \vdash \Theta, \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z})$, $i = 1, \ldots, l$, *then provable in G is a sequent*

$$\Gamma \vdash \Theta, \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}).$$

To prove this it is necessary to arrange the terms $g(\bar{t}^1), \ldots, g(\bar{t}^l)$ in nondecreasing order of their length and apply the induction hypothesis on l and Lemma 3. □

To return to the case under consideration, since the terms $g(\bar{t}^1), \ldots, g(\bar{t}^l)$ occur in the sequent $\Gamma_0 \vdash \Theta_0, \exists x\Phi_0$ and the terms $g(\bar{t}^{l+1}), \ldots, g(\bar{t}^m)$ do not, nor do the latter occur in the sequent $\Gamma_0 \vdash \Theta_0, \exists x\Phi_0, \Phi, \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots, \Psi(\bar{t}^l, g(\bar{t}^l), \bar{z})$. To establish that the last sequent is provable it is enough therefore to use the corollary of Lemma 3.

Case (2), where $\exists x\Phi_0$ is a marked ancestor of a formula $\exists\bar{x}\Psi(\bar{x}, g(\bar{x}), \bar{z})$, is treated similarly (even in a simpler way).

The case where a passage in D is performed according to Rule 10 is treated similarly to the case corresponding to Rule 7. □

Let us associate with every formula Φ in prenex normal form some $\exists$-formula Φ_H, called a Herbrand form of Φ, by the following rule. If Φ is an $\exists$-formula, then $\Phi_H = \Phi$; if Φ is of the form $\exists x_1 \ldots \exists x_n \forall y\Psi(\bar{x}, y, \bar{z})$ and g is an n-place function symbol not occurring in Φ, then $\Phi_H = (\exists x_1 \ldots \exists x_n\Psi(\bar{x}, g(\bar{x}), \bar{z}))_H$. It is established by induction on the number of universal quantifiers that this definition is correct.

Theorem (Herbrand). *Let* Φ *be a formula in prenex normal form and let* $\Phi_{\mathrm{H}} = \exists x_1 \ldots \exists x_n \Psi(\bar{x}, \bar{z})$ *be a Herbrand form of* Φ, *where* Ψ *is a quantifier-free formula. The formula* Φ *is provable if and only if there are sequences of terms* $\bar{t}^1 = t_1^1, \ldots, t_n^1; \ldots; \bar{t}^k = t_1^k, \ldots, t_n^k$ *such that a formula*

$$\Psi(\bar{t}^1, \bar{z}) \vee \ldots \vee \Psi(\bar{t}^k, \bar{z})$$

is provable.

PROOF. By induction (on the number of universal quantifiers) and the preceding theorem Φ is provable if and only if Φ_{H} is. To complete the proof we establish the following.

PROPOSITION 4. *A formula* $\Phi = \exists x_1 \ldots \exists x_n \Psi(\bar{x}, \bar{z})$, *where* Ψ *is a quantifier-free formula, is provable if and only if there is a sequence of n-collections of terms* $\bar{t}^1, \ldots, \bar{t}^k$ *such that a formula* $\Psi(\bar{t}^1, \bar{z}) \vee \ldots \vee \Psi(\bar{t}^k z)$ *is provable.*

PROOF. By invertibility (Proposition 31.1) the formula $\Psi(\bar{t}^1, \bar{z}) \vee \ldots \vee \Psi(\bar{t}^k, \bar{z})$ is provable if and only if a sequent $\vdash \Psi(\bar{t}^1, \bar{z}), \ldots, \Psi(\bar{t}^k, \bar{z})$ is provable.

Let that sequent be provable. Then a repeated application of the rule of introducing an existential quantifier yields a provable sequent $\vdash \exists \bar{x} \Psi(\bar{x}, \bar{z}), \ldots, \exists \bar{x} \Psi(\bar{x}, \bar{z})$. From this sequent via the rules of abbreviation we obtain a sequent $\vdash \exists \bar{x} \Psi(\bar{x}, \bar{z})$. This establishes sufficiency.

NECESSITY. Let D be a proof of a formula Φ in G with the property of the purity of variables. Let $\bar{t}^1, \ldots, \bar{t}^k$ be all n-collections of terms $\bar{t}$ such that there occurs a formula $\Psi(\bar{t}, \bar{z})$ in D. Notice that all formulas of D are ancestors of the formula Φ. Let a tree D^* be obtained from D by replacing each occurrence of the sequent $\Gamma_0 \vdash \Delta_0$ by a sequent $\Gamma_0 \vdash \Psi(\bar{t}^1, \bar{z}), \ldots, \Psi(\bar{t}^k, \bar{z}), \Delta_1$, where Δ_1 is obtained from Δ_0 by eliminating all formulas of the form $(\exists x_{s+1} \ldots \exists x_n \Psi(\bar{x}, \bar{z}))_{t_1, \ldots, t_s}^{x_1, \ldots, x_s}$, $0 \leqslant s \leqslant n$. It can be verified without difficulty that the resulting tree D^* is a quasi-derivation (of the sequent $\vdash \Psi(\bar{t}^1, \bar{z}), \ldots, \Psi(\bar{t}^k, \bar{z})$). Indeed, there are sequents at the tops obtained from the axioms by revisions. A passage corresponding to the propositional rules has corresponding passages according to the same rule (possibly with an abbreviation and interchanges). No quantifier rules are used in the tree D, except for Rule 7; the passages according to Rule 7 have corresponding trivial passages in D^*. The passages according to the structural rules have corresponding passages obtained by applying structural rules. So D^* is a quasi-derivation of the sequent $\vdash \Psi(\bar{t}^1, \bar{z}), \ldots, \Psi(\bar{t}^k, \bar{z})$ and necessity is established. □

The strength of the Herbrand theorem is in that the question of provability of an arbitrary formula is reduced to the question of provability of some effectively generated sequence of quantifier-free formulas. And it requires only propositional (and structural) rules to show the provability of a quantifier-free formula.

More precisely, let Φ be a quantifier-free formula and let $\Psi_0, \ldots, \Psi_n$ be all distinct atomic subformulas of Φ, then the propositional form of Φ is the formula Φ_P of the propositional calculus, which is obtained from Φ by substituting everywhere a propositional variable P_i, $i = 0, \ldots, n$, for a subformula Ψ_i.

PROPOSITION 5. *A quantifier-free formula Φ is provable in G if and only if its propositional form Φ_0 is provable in the propositional calculus.*

PROOF. Immediate from the property of being a subformula. □

34. THE CALCULI OF RESOLVENTS

The calculi of resolvents are used to search for a derivation in the propositional calculus and in the calculus of predicates. We begin with the propositional variant.

Formulas of propositional calculi of resolvents are propositional variables or their negations.

If Φ is a formula, then Φ^* is $\neg \Phi$ when Φ is a propositional variable and P when $\Phi = \neg P$.

The basic syntactical notion is that of a *list of formulas*. An empty list is denoted by $\varnothing$. The calculi of resolvents have the same rules of inference and differ only in axioms. If $\Gamma_0; \ldots; \Gamma_n$ are lists of formulas, then $R_P(\Gamma_0; \ldots; \Gamma_n)$ denotes the (*propositional*) *calculus of resolvents* whose axioms are the lists $\Gamma_0; \ldots; \Gamma_n$.

The *rules of inference* of the calculi of resolvents are:

$$1.\ \frac{\Gamma, \Phi \quad \Theta, \Phi^*}{\Gamma, \Theta}, \qquad 2.\ \frac{\Gamma, \Phi, \Psi, \Theta}{\Gamma, \Psi, \Phi, \Theta}, \qquad 3.\ \frac{\Gamma, \Phi, \Phi}{\Gamma, \Phi}.$$

The notion of (tree form) *proof* is defined in the usual way. If Γ is a nonempty list of formulas, then $\wedge\Gamma$ denotes a conjunction of formulas of Γ. $\wedge\Gamma$ is a formula of the propositional calculus, but generally speaking it is not a formula of the calculus of resolvents.

LEMMA 1. *If D is a proof of a list Γ in $R_P(\Gamma_0; \ldots; \Gamma_n)$ and Γ_n occurs at the top of D, then for any list Γ' in $R_P(\Gamma_0; \ldots; \Gamma_{n-1}; \Gamma', \Gamma_n)$ a list Γ', Γ is provable.*

PROOF. By induction on the number of lists of the tree D. If $D = \Gamma_n$, then $\Gamma = \Gamma_n$ and Γ', Γ is a proof in $R_P(\Gamma_0; \ldots; \Gamma_{n-1}; \Gamma', \Gamma_n)$.

Let $D = \dfrac{D_0 D_1}{\Gamma}$ and suppose that the last passage is $\dfrac{\Gamma^0, \Phi\Gamma^1, \Phi^*}{\Gamma^0, \Gamma^1}$, then by the induction hypothesis there are proofs D_0', D_1' in $R_P(\Gamma_0; \ldots; \Gamma_{n-1}; \ldots; \Gamma', \Gamma_n)$ of lists Γ', Γ^0, Φ (or Γ^0, Φ if Γ_n does not occur at the top of D_0) and $\Gamma', \Gamma^1, \Phi^*$ (or Γ^1, Φ^* if Γ_n does not occur in D_1) respectively. Since Γ_n occurs at the top of D_0 or at the top of D_1, then at least one of the trees

$$\frac{D_0' \quad D_1'}{\Gamma', \Gamma^0, \Gamma', \Gamma^1}, \qquad \frac{D_0' \quad D_1'}{\Gamma', \Gamma^0, \Gamma^1}, \qquad \frac{D_0' \quad D_1'}{\Gamma^0, \Gamma', \Gamma^1}$$

is a proof in $R_P(\Gamma_0; \ldots; \Gamma_{n-1}, \Gamma', \Gamma_n)$. From the final list we easily obtain Γ', Γ with the aid of the structural rules.

If the last passage in the tree D is effected by Rules 2 and 3, the induction step is obvious. □

We now prove a statement relating the calculus of resolvents to provability in the propositional calculus.

PROPOSITION 1. *If $\Gamma_0; \ldots; \Gamma_n$ are nonempty lists of formulas (of the calculus of resolvents), then the formula $\bigvee_{i=0}^{n} (\wedge\Gamma_i)$ is provable in the propositional calculus if and only if the empty list of formulas $\varnothing$ is provable in the calculus $R_P(\Gamma_0; \ldots; \Gamma_n)$.*

PROOF. Let D be a tree of lists of formulas such that its tops contain nonempty lists of formulas $\Theta_0; \ldots; \Theta_k$, each passage is a passage according to one of the rules of inference in the calculus of resolvents and Θ is the final (possibly empty) list of formulas.

We prove that then a sequent $\Theta \vdash \bigvee_{i=0}^{k} (\wedge\Theta_i)$ is provable in the propositional calculus. We shall proceed by induction on the number of lists of formulas in the tree D.

Let D consist of a single (nonempty) list Θ, then the sequent $\Theta \vdash \wedge\Theta$ is obviously provable in the propositional calculus.

Let the tree D be of the form $\frac{D_0 \quad D_1}{\Theta}$; $\Theta_0^0; \ldots; \Theta_{k_0}^0$ be the lists at the tops of D_0; $\Theta_0^1; \ldots; \Theta_k^1$ be the lists at the tops of D_1. Let the final passage be

$$\frac{\Theta_0, \Phi \quad \Theta_1, \Phi^*}{\Theta}$$

(then $\Theta = \Theta_0, \Theta_1$). By the induction hypothesis the sequents $\Theta_0, \Phi \vdash \Phi^0$ and $\Theta_1, \Phi^* \vdash \Phi^1$, where $\Phi^0 = \bigvee_{i=0}^{k} (\wedge\Theta_i^0)$ and $\Phi^1 = = \bigvee_{i=0}^{k_1} (\wedge\Theta_i^1)$, are provable in the propositional calculus. Then the tree

$$\dfrac{\vdash \Phi \vee \Phi^* \quad \dfrac{\Theta_0, \Phi \vdash \Phi^0}{\Theta_0, \Phi \vdash \Phi^0 \vee \Phi^1} \quad \dfrac{\Theta_1, \Phi^* \vdash \Phi^1}{\Theta_1, \Phi^* \vdash \Phi^0 \vee \Phi^1}}{\Theta_0, \Theta_1 \vdash \Phi^0 \vee \Phi^1}$$

is a quasi-derivation of the required sequent for the tree D.

The case where the last passage in the tree D corresponds to the structural Rule 2 or 3 is obvious. It follows from the proved statement that if the empty list of formulas is provable in $R_P(\Gamma_0; \ldots; \Gamma_n)$, then the formula $\bigvee_{i=0}^{n} (\wedge\Gamma_i)$ is provable in the propositional calculus.

To prove the converse we shall use the propositional variant G_P of the calculus G. We show by induction on the number of conjunctions in a sequent

$$\vdash \wedge\Theta_0, \ldots, \wedge\Theta_k \tag{*}$$

that if that sequent is provable in G_P, then the empty list is provable in $R_P(\Theta_0; \ldots; \Theta_k)$.

Let the sequent (*) contain no conjunction sign. Then it has the form $\vdash \Phi_0, \ldots, \Phi_k$, where Φ_i are propositional variables or their negations. Such a sequent is provable in G_P if and only if there are $i, j \leqslant k$ such that $\Phi_i = \Phi_j^*$ and so

$$\frac{\Phi_j \quad \Phi_j^*}{\varnothing}$$

is a proof in $R_P(\Phi_0; \ldots; \Phi_k)$.

Let the statement be true for sequents of the form (*) with the number of $\wedge$ signs less than n. Let a sequent (*) have n $\wedge$ signs and let $\Theta_k = \Theta_k^0, \Theta_k^1$, where Θ_k^0 and Θ_k^1 are nonempty lists of formulas. By invertibility, if a sequent (*) is provable, then so are the sequents $\vdash \wedge\Theta_0, \ldots, \wedge\Theta_{k-1}, \wedge\Theta_k^0$ and $\vdash \wedge\Theta_0, \ldots, \wedge\Theta_{k-1}, \wedge\Theta_k^1$. By the induction hypothesis the empty list $\varnothing$ is provable in $R_P(\Theta_0; \ldots; \Theta_{k-1}; \Theta_k^0)$ and $R_P(\Theta_0; \ldots; \Theta_{k-1}; \Theta_k^1)$. Let D_0 and D_1 be the corresponding proofs. If Θ_k^1 does not occur at the tops of the tree D_1, then D_1 is a proof (of the list $\varnothing$) in $R_P(\Theta_0; \ldots; \Theta_{k-1})$ and all the more in $R_P(\Theta_0; \ldots; \Theta_{k-1}; \Theta_k)$. If Θ_k^1 does occur at the tops of D_1, then by Lemma 1 there is a proof D_1' of the list Θ_k^0 in $R_P(\Theta_0; \ldots; \Theta_{k-1}; \Theta_k = \Theta_k^0, \Theta_k^1)$. Substituting a tree D_0' for all tops of the form Θ_k^0 in D_0 yields a proof of the empty list in $R_P(\Theta_0; \ldots; \Theta_k)$.

To return to the proof of the required statement. By invertibility the formula $\bigvee_{i=0}^{n} (\wedge\Gamma_i)$ is provable in G_P if and only if so is the sequent $\vdash \wedge\Gamma_0, \ldots, \wedge\Gamma_n$. According to the statement just proved, it follows from the provability of the sequent $\vdash \wedge\Gamma_0, \ldots, \wedge\Gamma_n$ that the empty list of formulas $\varnothing$ is provable in $R_P(\Gamma_0; \ldots; \Gamma_n)$. □

We now proceed to study the *calculi of resolvents* for the calculus of predicates.

Formulas of a calculus of resolvents are atomic formulas of the calculus G or their negations. For a formula Φ we define Φ^* as above. The rules of inference are Rules 1, 2, 3 and Rule

$$4. \frac{\Gamma}{(\Gamma)_t^x},$$

where $\bar{x} = x_1, \ldots, x_k$ is a list of distinct variables and $\bar{t} = t_1, \ldots, t_k$ is a list of terms.

Calculi of resolvents differ in axioms. A calculus of resolvents with axioms (with lists) $\Gamma_0; \ldots; \Gamma_n$ is denoted by $R(\Gamma_0; \ldots; \Gamma_n)$. The relation of a calculus of resolvents to provability in the calculus of predicates is established by the following statement.

PROPOSITION 2. *Let* $\Phi = \exists x_1 \ldots \exists x_m \left(\bigvee_{i=0}^{n} (\wedge \Gamma_i) \right)$ *be a closed formula of the calculus of predicates and let* Γ_i, $i = 0, \ldots, n$, *be nonempty lists of atomic formulas or of their negations. A formula* Φ *is provable in the calculus of predicates if and only if so is the empty list of formulas in the calculus of resolvents* $R(\Gamma_0; \ldots; \Gamma_n)$.

PROOF. Let Φ be a formula provable in G. Then by Proposition 31.3′ there are collections of terms $\bar{t}^1 = t_1^1, \ldots, t_m^1; \ldots; \bar{t}^k = t_1^k, \ldots, t_m^k$ such that the following sequent is provable

$$\vdash \left(\bigvee_{i=0}^{n} (\wedge \Gamma_i) \right)^{\bar{x}}_{\bar{t}^1}, \ldots, \left(\bigvee_{i=0}^{n} (\wedge \Gamma_i) \right)^{\bar{x}}_{\bar{t}^k}.$$

The provability of this sequent is equivalent to the provability of the formula

$$\Phi' = \bigvee_{\substack{0 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant k}} (\wedge \Gamma_i)^{\bar{x}}_{\bar{t}j}.$$

By Proposition 33.4 Φ' is provable if and only if so is the propositional formula Φ'_p. Using Proposition 1 we conclude from the provability of Φ'_p in the propositional calculus that in the calculus of resolvents $R(\ldots; (\Gamma_i)^{\bar{x}}_{\bar{t}j}; \ldots)$ the empty list is provable making use of Rules 1 to 3 only. (To do this it is necessary to replace the propositional variables by the corresponding elementary formulas in the proof of the empty list in the propositional calculus of resolvents associated with the formula Φ'_p.) But since lists $(\Gamma_i)^{\bar{x}}_{\bar{t}j}$ are obtained from lists Γ_i by Rule 4, it follows that the empty list is provable in $R(\Gamma_0; \ldots; \Gamma_n)$.

As in Proposition 1, to prove the converse we shall establish the following statement: if D is a proof of a list Θ in $R(\Gamma_0; \ldots; \Gamma_n)$

and $\bar{x} = x_1, \dots, x_m$ is a list of all variables in the formulas of lists $\Gamma_0; \dots; \Gamma_n$, then there are collections of terms $\bar{t}^i = t^i_1, \dots, t^i_m$, $i = 1, \dots, k$, such that a sequent $\Theta \vdash \bigvee\limits_{i=1}^{k}\left(\bigvee\limits_{j=0}^{n}(\wedge(\Gamma_j)^{\bar{x}}_{\bar{t}}i)\right)$ is provable in the calculus G.

We proceed by induction on the number of lists in the proof D. When D is simply a list Γ_i, the following tree is a quasi-derivation of the required sequent:

$$\frac{\Gamma_i \vdash \wedge\Gamma_i}{\Gamma_i \vdash \bigvee\limits_{j=1}^{k}(\wedge\Gamma_j)}.$$

Let the proof D be of the form $\frac{D'}{\Theta}$ and let the last passage be

$$\frac{\Theta'}{\Theta}, \text{ where } \Theta = (\Theta')^u_t.$$

By the induction hypothesis a sequent

$$C = \Theta' \vdash \bigvee_{i=1}^{k}\left(\bigvee_{j=0}^{n}(\wedge(\Gamma_j)^{\bar{x}}_{\bar{t}}i)\right)$$

is provable for some collections of terms $\bar{t}^1, \dots, \bar{t}^k$ in the calculus of predicates.

It is obvious that the provability of the sequent C implies that of a sequent $C' = (C)^u_t$ (it is necessary to take a proof of the sequent C in G and substitute $(D)^u_t$), but then a sequent $C' = \Theta' \vdash \bigvee\limits_{i=1}^{k}\left(\bigvee\limits_{j=0}^{n}(\wedge(\Gamma_j)^{\bar{x}}_{\bar{t}'}j)\right)$, where $\bar{t}'^j = (\bar{t}^j)^u_t$, is provable.

The cases where the last passage in the proof D is performed according to Rule 1, 2 or 3 are treated as in Proposition 1. So if the empty list $\varnothing$ is provable in $R(\Gamma_0; \dots; \Gamma_n)$, then there are collections of terms $\bar{t}^1; \dots; \bar{t}^k$ such that a sequent $\vdash \bigvee\limits_{i=1}^{k}\left(\bigvee\limits_{j=0}^{n}(\wedge(\Gamma_j)^{x}_{t}i)\right)$ is provable. Then a sequent

$\vdash \left(\bigvee_{j=0}^{n} (\wedge\Gamma_j)\right)^{\bar{x}}_{\bar{t}^1}, \ldots, \left(\bigvee_{j=0}^{n} (\wedge\Gamma_j)\right)^{x}_{\bar{t}^k}$ is provable. It is easy to derive from the provability of such a sequent that a sequent

$$\vdash \exists x_1 \ldots \exists x_m \left(\bigvee_{j=0}^{n} (\wedge\Gamma_j)\right)$$

is provable too. □

We now show how to reduce the question of the provability in G of an arbitrary formula Φ of G to the question of the provability of the empty list in a suitable calculus of resolvents.

If Φ contains free variables $z_0, \ldots, z_n$, then it is easy to verify using the corollary of Proposition 31.2 that Φ is provable if and only if so is the universal closure $\Phi^0 = \forall z_0 \ldots \forall z_n \Phi$ of the formula Φ.

Let Φ^0 be a closed formula. Then we can find for it effectively an equivalent formula Φ^1 in prenex normal form. By the Herbrand theorem the provability of the formula Φ^1 (and hence of the formulas Φ^0 and Φ) is equivalent to the provability of the Herbrand form Φ^1_{H} of Φ^1. The matrix of Φ^1_{H} is in disjunctive normal form, i. e. has the form $\bigvee_{i=0}^{n} (\wedge\Gamma_i)$, where Γ_i are some lists of atomic formulas or of their negations. But then Φ^1_{H} is a closed $\exists$-formula and hence by Proposition 2 its provability is equivalent to the derivability of the empty list $\varnothing$ in the calculus of resolvents $R(\Gamma_0, \ldots, \Gamma_n)$.

From what we have just proved, from Theorem 23.11 and Theorem 32.2 we see that the question of provability of an arbitrary formula Φ in the calculus of predicates reduces to the question of provability of the empty list in a suitable calculus of resolvents.

Machine realizations of a search for the provability of the empty list in a calculus of resolvents make use of various deterministic (and sometimes also nondeterministic) methods of successive transformation of lists so that all provable lists are obtained in such transformations. Such methods are called *strategies* of a search. Any discussion of strategies is beyond the scope of this textbook.

To get at least a feeling of what problems may arise here the reader should prove the following statement.

PROPOSITION 3. *There is an algorithm which finds out from two formulas,* Φ *and* Ψ, *of a calculus of resolvents if there are collections of terms* $\bar{t} = t_1, \ldots, t_n$ *such that formulas* $(\Phi)^{\bar{x}}_{\bar{t}}$ *and* $(\Psi)^{\bar{x}}_{\bar{t}}$ *coincide and if there are, then it finds such a universal collection* $\bar{t}$.

Universality means that for any collection $\bar{t}\,'$ such that $(\Phi)^{\bar{x}}_{\bar{t}'} = (\Psi)^{\bar{x}}_{\bar{t}'}$ there is a collection of terms $\bar{t}\,'' = t''_0, \ldots, t''_k$ corresponding to a list $\bar{u} = u_0, \ldots, u_k$ of free variables of the terms of $\bar{t}$ such that $\bar{t}\,' = (\bar{t})^{\bar{u}}_{\bar{t}''}$. □

Chapter 7

ALGORITHMS AND RECURSIVE FUNCTIONS

35. NORMAL ALGORITHMS AND TURING MACHINES

In the preceding chapters we have repeatedly referred to an algorithm $\mathfrak{A}$ operating on some set of objects X, understanding by this an exact prescription determining from any object $a \in X$ some well-defined sequence of elementary operations performing which we either never terminate the process (of computation) or the process terminates and we obtain an object $\mathfrak{A}(a)$ called the *value of* $\mathfrak{A}$ *at* a or the process terminates without yielding a value. If a process determined by an algorithm $\mathfrak{A}$ from an element a does not terminate or terminates without yielding a value, then it is said that $\mathfrak{A}$ *is not applicable to* a. Examples of algorithms are the rules of addition, multiplication and division operating on the set of pairs of natural numbers. Notice that the division algorithm is not applicable to a pair of natural numbers $\langle n, m\rangle$, if n is not even divisible by m. Another example is the algorithm, described in Sec. 20, for finding from a formula of the calculus of predicates an equivalent formula in prenex normal form. The number of elementary operations required for a value of an algorithm to be obtained may be very large. At this level of study, however, we shall abstract from practical possibilities of realizing algorithms and proceed from the assumption that we have an unlimited store of time and materials when realizing a process of computation. This assumption is called the *principle of potential realizability*.

As a rule, an intuitive understanding is enough to establish whether or not a given prescription is an algorithm. One cannot do without a precise definition of an algorithm, however, if one attempts to prove that there is no single effective procedure (an algorithm) for solving a certain class of problems. But is it possible to find such a mathematical definition for the notion of algorithm which would both embrace the various already existing algorithms and effective procedures accumulated by mathematical and computational practice and ensure that any future intuitively acceptable algorithm does not demolish that definition? Posed so broadly, this question could hardly be given a positive answer. However, the actual development of mathematics has led to a satisfactory solution (it would be more precise to say settlement) of this problem. Namely, several formalizations of the notion of algorithm were proposed differing in their scope, collection of admissible elementary operations and possibilities of composing prescriptions (programs) for computation. The study of these formalizations has shown that they possess the properties of being closed under all possible combinations (superpositions, iterations and so on), have a great power of reproducing to a reasonable degree of similarity (adequacy) all known algorithmic procedures and methods. The most essential to the justification of the definitions has turned out to be the coincidence of classes of computable functions for all these notions. Therefore at least the concept of (algorithmically) computable function (with natural arguments and values) has turned out to be invariantly defined and this is quite enough for theoretical purposes. The existence of a number of different definitions (strengthenings) of the notion of algorithm has its advantages as well, since it is convenient to use different ad hoc definitions in solving different problems. There is a similar phenomenon in programming: the existing multiplicity of programming languages is to a large extent due to the multiplicity of problems facing human computers and programmers. In this section we shall give definitions for two different classes of algorithms, *normal algorithms* and *Turing machines*. No detailed study of these concepts is envisaged here. We restrict ourselves to precise definitions, examples and formulations of the main statement about the relation of these concepts. In the subsequent sections we shall study in more detail a class of computable functions and give it yet another (already a third) definition.

Before proceeding to precise definitions consider an example.

EXAMPLE 1. Construct an algorithm $\mathfrak{A}$ operating on the set of the words of the alphabet of PC and computing the characteristic function of the set of formulas of PC, i. e. an algorithm $\mathfrak{A}$ such that $\mathfrak{A}(\alpha) = 1$ if α is a formula of PC and $\mathfrak{A}(\alpha) = 0$ otherwise.

Let φ be a letter distinct from all the letters of the alphabet of

PC. The following transformations will be performed with each word α in the alphabet of PC:

1. We replace every occurrence of a propositional variable in the word α by a letter φ; let the word obtained be α_1.

2. We construct a sequence of words $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that every word α_{i+1}, $0 < i < n$, is obtained from a word α_i by replacing one subword of the form $\neg\varphi$, $(\varphi \wedge \varphi)$, $(\varphi \vee \varphi)$ or $(\varphi \rightarrow \varphi)$ by φ; and the word α_n contains no subword of this form.

3. If α_n coincides with φ, then we set $\mathfrak{A}(\alpha) = 1$. If α_n is distinct from φ, then we set $\mathfrak{A}(\alpha) = 0$.

Letting the reader see for himself that this algorithm is applicable to any word and that it is correct, we note that the elementary operations in this algorithm are successive replacements of the occurrences of subwords of special form by other words. An important feature of the algorithm is a possible ambiguity (indeterminacy) in the process of computation, the sequence of words $\alpha_1, \alpha_2, \ldots, \alpha_n$ not being determined uniquely from α (although the number n is easily seen to be uniquely defined). The concepts of normal algorithm and Turing machine defined below also have replacements of subwords by words as elementary operations, but the sequence of the operations is uniquely defined.

Each of the algorithms defined below operates on the set of all words of some alphabet B. A part of the letters of that alphabet plays an auxiliary technical role. To distinguish the essential part A of $B (A \subseteq B)$, therefore, any algorithm $\mathfrak{A}$ operating on the set of words of B is said to be an *algorithm over* A.

Algorithms $\mathfrak{B}$ and $\mathfrak{C}$ over A are said to be *equivalent with respect to* A if for any word α of A two conditions hold:

(a) if $\mathfrak{B}$ is applicable to a word α of the alphabet A, then $\mathfrak{C}$ is applicable to α and $\mathfrak{B}(\alpha) = \mathfrak{C}(\alpha)$.

(b) the condition obtained from (a) by interchanging $\mathfrak{B}$ and $\mathfrak{C}$.

We proceed to formulate the concept of normal algorithm proposed by A. A. Markov. In what follows we let A be a finite alphabet.

DEFINITION. *A schema S in an alphabet A* is an ordered collection of triples

$$\langle \langle \alpha_1, \beta_1, \delta_1 \rangle, \ldots, \langle \alpha_n, \beta_n, \delta_n \rangle \rangle,$$

in which the first two elements α_i, β_i are words of A and the third element, δ_i, is in the set $\{0, 1\}$. A *normal algorithm* in A is a pair $\langle A, S\rangle$ consisting of the alphabet A and a schema S in the alphabet A.

Let α be a word in A, let $\mathfrak{A} = \langle A, S\rangle$ be a normal algorithm and let $S = \langle\langle\alpha_1, \beta_1, \delta_1\rangle, \ldots, \langle\alpha_n, \beta_n, \delta_n\rangle\rangle$. If none of the words $\alpha_1, \ldots, \alpha_n$ is a subword of α, then we shall say that the word α *does not lend itself to the algorithm* $\mathfrak{A}$. If i_0 is the least number for which α_{i0} is a subword of α and if β is the result of the replacement of the first occurrence of α_{i0} in α by a word β_{i0}, then we shall say that $\mathfrak{A}$ *simply converts* α *into* β if $\delta_{i_0} = 0$ (we write $\mathfrak{A}\colon \alpha \vdash \beta$) and that $\mathfrak{A}$ *finally converts* α *into* β if $\delta_{i_0} = 1$ (we write $\mathfrak{A}\colon \alpha \vdash \cdot\beta$). Of course, it is assumed that the signs $\vdash$ and $\cdot$ are exterior to the alphabet A. If $\mathfrak{A}$ simply or finally converts α into β, then we say that $\mathfrak{A}$ *converts* α *into* β. We shall say that $\mathfrak{A}$ *transforms a word* α *into a word* β (we write $\mathfrak{A}(\alpha) = \beta$) if there is a sequence $\gamma_0, \ldots, \gamma_k$ of words of A such that the following conditions hold:

(a) $\gamma_0 = \alpha$ and $\gamma_k = \beta$;

(b) if $k = 0$, then α does not lend itself to $\mathfrak{A}$;

(c) $\mathfrak{A}$ simply converts γ_i into γ_{i+1} for $i < k - 1$;

(d) if $k > 0$ $\mathfrak{A}\colon \gamma_{k-1} \vdash \cdot\gamma_k$ does not hold, then $\mathfrak{A}\colon \gamma_{k-1} \vdash \cdot\gamma_k$ and γ_k does not lend itself to $\mathfrak{A}$.

If a sequence $\gamma_0, \ldots, \gamma_k$ satisfies conditions (a) to (c), and the condition $\mathfrak{A}\colon \gamma_{k-1} \vdash \gamma_k$ ($\mathfrak{A}\colon \gamma_{k-1} \vdash \cdot\gamma_k$), then we shall write $\mathfrak{A}\colon \alpha \models \beta$ ($\mathfrak{A}\colon \alpha \models \cdot\beta$).

It follows from the definition that if a normal algorithm converts a word α into a word β, then β is uniquely determined from $\mathfrak{A}$ and α. If $\mathfrak{A}$ finally converts α into β, then $\mathfrak{A}$ cannot simply convert α into β. It is also clear that if α does not lend itself to $\mathfrak{A}$, then $\mathfrak{A}$ does not convert α into any word. From these properties we see that if a normal algorithm $\mathfrak{A}$ transforms a word α into a word β, then β is uniquely determined from $\mathfrak{A}$ and α (this justifies our writing $\mathfrak{A}(\alpha) = \beta$). If a normal algorithm does not transform α into any word, then we say that the algorithm $\mathfrak{A}$ *is not applicable to the word* α. Notice that if a normal algorithm $\mathfrak{A} = \langle A, S\rangle$ is not applicable to a word α of A, then there is an infinite sequence of words $\gamma_0 = \alpha, \gamma_1, \gamma_2, \ldots, \gamma_n, \ldots$ for which $\mathfrak{A}\colon \gamma_i \vdash \gamma_{i+1}$, $i \in \omega$.

In what follows the triple $\langle\alpha, \beta, \delta\rangle$ of a schema S in A will be represented more graphically $\alpha \to \beta$ if $\delta = 0$ and $\alpha \to \cdot\beta$ if $\delta = 1$, assuming, of course, that → and · are exterior to A. The schema S is given by enumerating such words.

EXAMPLE 2. Let $A = \{Q_0, Q_1, \wedge, \vee, \neg, (,), a\}$. Consider a normal algorithm $\mathfrak{A} = \langle A, S\rangle$ with the following schema:

(1) $aQ_0 \to Q_0 a$,
(2) $aQ_1 \to Q_1 a$,
(3) $a\wedge \to \wedge a$,
(4) $a\vee \to \vee a$,
(5) $a\neg \to \neg a$,
(6) $a(\to (a$,
(7) $a) \to)a$,
(8) $a \to \cdot \vee Q_0)$,
(9) $\Lambda \to (a$.

It will be left for the reader to verify that if Φ is a formula of PC in the alphabet $A \setminus \{a\}$, then $\mathfrak{A}(\Phi) = (\Phi \vee Q_0)$. To illustrate how the algorithm works we write out a number of successive substitutions realized by the algorithm $\mathfrak{A}$ beginning with the formula $(Q_0 \wedge \neg Q_1)$. The part of the word to be replaced at a given stage is given in a bold type:

$$(Q_0 \wedge \neg Q_1) \to (\boldsymbol{a(}Q_0 \wedge \neg Q_1) \to ((\boldsymbol{aQ_0} \wedge \neg Q_1) \to$$
$$\to ((Q_0\boldsymbol{a \wedge} \neg Q_1) \to ((Q_0 \wedge \boldsymbol{a \neg} Q_1) \to ((Q_0 \wedge \neg \boldsymbol{aQ_1}) \to$$
$$\to ((Q_0 \wedge \neg Q_1 \boldsymbol{a)} \to ((Q_0 \wedge \neg Q_1)\boldsymbol{a} \to \cdot ((Q_0 \wedge \neg Q_1) \vee Q_0).$$

At first sight the definition of a normal algorithm does not allow us to hope for any universality of that concept. A little experience is enough, however, to see the really ample possibilities of normal algorithms. To illustrate, the class of normal algorithms is closed under a composition.

Let $\mathfrak{A}_0 = \langle A, S_0\rangle, \mathfrak{A}_1 = \langle A, S_1\rangle$ be two normal algorithms in an alphabet A. A normal algorithm $\mathfrak{B}$ over A is said to be the *composition of algorithms* $\mathfrak{A}_0$ *and* $\mathfrak{A}_1$ if for any word α in A $\mathfrak{B}$ is applicable to α if and only if $\mathfrak{A}_0$ is applicable to α and $\mathfrak{A}_1$ is applicable to $\mathfrak{A}_0(\alpha)$, and then $\mathfrak{B}(\alpha) = \mathfrak{A}_1(\mathfrak{A}_0(\alpha))$.

PROPOSITION 1. *For any two normal algorithms* $\mathfrak{A}_0$ *and* $\mathfrak{A}_1$ *in an alphabet* A *there is a normal algorithm* $\mathfrak{B}$ *over* A *which is the composition of* $\mathfrak{A}_0$ *and* $\mathfrak{A}_1$.

PROOF. It is assumed that the alphabet A does not contain the letters $0, 0', 1$ and $1'$. The algorithm $\mathfrak{B}$ we are constructing is in the alphabet $A \cup \{0, 0', 1, 1'\}$. For further purposes, it may be assumed without loss of generality that the schemata S_0 and S_1 of $\mathfrak{A}_0$ and $\mathfrak{A}_1$ respectively contain triples of the form $\langle \wedge, \beta, 1 \rangle$. Indeed, it is easy to verify that if we add another triple, $\langle \Lambda, \Lambda, 1 \rangle$, as the last one in the schema S_i of the algorithm $\mathfrak{A}_i$, $i = 0, 1$, then the resulting algorithm $\mathfrak{A}_i'$ will be equivalent to $\mathfrak{A}_i$ over A; therefore the composition of the algorithms $\mathfrak{A}_0'$ and $\mathfrak{A}_1'$ will be the composition of the algorithms $\mathfrak{A}_0$ and $\mathfrak{A}_1$ as well.

Let S_0^0 be an ordered sequence of triples obtained from the schema S_0 by replacing each triple $\langle \alpha, \beta, \delta \rangle$ by a triple $\langle \alpha, \beta, \delta \rangle^0$, where

$$\langle \alpha, \beta, \delta \rangle^0 = \begin{cases} \langle 0'\alpha, 0\beta, 0 \rangle & \text{if} \quad \delta = 0 \\ \langle 0'\alpha, 1\beta, 0 \rangle & \text{if} \quad \delta = 1. \end{cases}$$

Let S_1^1 be an ordered sequence of triples obtained from S_1 by replacing each triple $\langle \alpha, \beta, \delta \rangle$ by a triple $\langle \alpha, \beta, \delta \rangle^1$, where

$$\langle \alpha, \beta, \delta \rangle^1 = \begin{cases} \langle 1'\alpha, 1\beta, 0 \rangle & \text{if} \quad \delta = 0 \\ \langle 1'\alpha, \ \ \beta, 1 \rangle & \text{if} \quad \delta = 1. \end{cases}$$

Let $A = \{a_0, a_1, \ldots, a_k\}$. Then a schema S of $\mathfrak{B}$ is the following ordered sequence (with the external brackets $\langle\ \rangle$ omitted):

$$\begin{aligned} &\langle a_0 0, 0a_0, 0 \rangle, \ldots, \langle a_k 0, 0a_k, 0 \rangle, \\ &\qquad S_0^0, \langle 0'a_0, a_0 0', 0 \rangle, \ldots, \langle 0'a_k, a_k 0', 0 \rangle, \langle 0, 0', 0 \rangle, \\ &\quad \langle a_0 1, 1a_0, 0 \rangle, \ldots, \langle a_k 1, 1a_k, 0 \rangle, S_1^1, \langle 1'a_0, a_0 1', 0 \rangle, \ldots \\ &\qquad\qquad\qquad \ldots, \langle 1'a_k, a_k 1', 0 \rangle, \langle 1, 1', 0 \rangle, \langle \Lambda, 0', 0 \rangle. \end{aligned}$$

To write this more graphically "in a column",

$$\begin{array}{rcll} \xi 0 & \to & 0\xi & \quad \xi \in A, \\ & S_0^0, & & \\ 0'\xi & \to & \xi 0', & \quad \xi \in A, \\ 0 & \to & 0' & \\ \xi 1 & \to & 1\xi, & \quad \xi \in A, \\ & S_1^1, & & \\ 1'\xi & \to & \xi 1', & \quad \xi \in A, \\ 1 & \to & 1', & \\ \Lambda & \lhd & 0. & \end{array}$$

The normal algorithm $\mathfrak{B} = \langle A \cup \{0, 0', 1, 1'\}, S\rangle$ is precisely the composition of the algorithms $\mathfrak{A}_0$ and $\mathfrak{A}_1$. Leaving a complete check of the details to the reader, we list the main points in the work of the algorithm $\mathfrak{B}$.

Let α be a word in A. Then

(1) $\mathfrak{B}\colon \alpha \vdash 0\alpha$;

(2) *if* $\mathfrak{A}_0\colon \alpha \vdash \alpha'$, *then* $\mathfrak{B}\colon 0'\alpha \models 0'\alpha'$;

(3) $\mathfrak{B}\colon 0\alpha \vdash 0'\alpha$;

(4) *if* $\mathfrak{A}_0\colon \alpha \vdash \cdot\alpha'$, *then* $\mathfrak{B}\colon 0'\alpha \models 1\alpha'$;

(5) $\mathfrak{B}\colon 1\alpha \vdash 1'\alpha$;

(6) *if* $\mathfrak{A}_1\colon \alpha \vdash \alpha'$, *then* $\mathfrak{B}\colon 1'\alpha \models 1'\alpha'$;

(7) *if* $\mathfrak{A}_1\colon \alpha \vdash \cdot\alpha'$, *then* $\mathfrak{B}\colon 1'\alpha \models \cdot\alpha'$. ☐

We now formulate the fundamental principle of the "universality" of normal algorithms.

NORMALIZATION PRINCIPLE. *Any algorithm over a finite alphabet A is equivalent with respect to A to some normal algorithm over A.*

The reasons for the validity of this principle, which is not a mathematical statement, were discussed from the very beginning of the section as the material was presented.

It may seem that the requirement that the algorithm should be finite prevents us from treating normal algorithms as an adequate representation of the concept of algorithm in mathematics. This is not an important limitation, however. The thing is that if some algorithm $\mathfrak{B}$ operates on a set M, then the elements of M and those of $\mathfrak{B}(m)$ must be effectively defined, and hence the elements of M and $\mathfrak{B}(m)$ have a finite number of integral invariants, it being possible to evaluate those invariants and reconstruct an object from them using some "coding" and "decoding" algorithms. It is thus enough to restrict oneself to algorithms operating on sequences of natural numbers and producing as values also sequences of natural numbers. And sequences of natural numbers can be coded in natural numbers themselves (for example, by assigning to the sequence $n_0, \ldots, n_k$ a number $2^{n_0+1} \times 3^{n_1+1} \cdot \ldots \cdot p_k^{n_k+1}$, where $p_0, p_1, \ldots, p_k$ are prime numbers written out in ascending order). Therefore the question of finding a more precise definition of the concept of algorithm reduces to the question of describing a class of functions $f\colon X \to \omega$, where

$X \subseteq \omega^n$, for which there is a computing algorithm in the intuitive sense mentioned at the beginning of this section.

Throughout the following, by a *partial function* we mean a mapping $f: X \to \omega$, where $X \subseteq \omega^n$ for some $n \in \omega$. A partial function $f: X \to \omega$, $X \subseteq \omega^n$, is said to be *computable* if there is an algorithm $\mathfrak{B}$ operating on ω^n, not applicable to n-tuples $\bar{a} \notin X$, for which $\mathfrak{B}(\bar{a}) = f(\bar{a})$, $\bar{a} \in X$. To represent a natural number m we shall use not the ordinary decimal notation, but a simpler notation, $11 \ldots 1$, where the number of units is $m + 1$. Such a number will further be called the notation of a number m and denoted by $\underline{m}$. A collection of numbers $\langle m_1, \ldots, m_n \rangle$ is represented by a word $\underline{\alpha} = \underline{m}_1 0 \underline{m}_2 0, \ldots, 0 \underline{m}_n$ and called the *notation of an n-tuple* $\alpha = \langle m_1, \ldots, m_n \rangle$.

DEFINITION. A partial function $f: X \to \omega$, $X \subseteq \omega^n$, is said to be *normally computable* if there is a normal algorithm $\mathfrak{A} = \langle A, S \rangle$ such that $0, 1 \in A$ for any n-tuple $\langle m_1, \ldots, m_n \rangle \in \omega$ $\langle m_1, \ldots, m_n \rangle \in X \Leftrightarrow \mathfrak{A}$ is applicable to the notation $\langle m_1, \ldots, m_n \rangle$ and $\mathfrak{A}(\underline{\alpha}) = f(\underline{\alpha})$ for $\alpha \in X$. Such an algorithm $\mathfrak{A}$ is called a *normal algorithm computing a function f.*

The normalization principle for partial functions will now read: *the class of computable partial functions coincides with the class of normally computable partial functions.*

EXAMPLE 3. Construct a normal algorithm $\mathfrak{A}$ computing the function x^2. Let $\mathfrak{A} = \langle A, S \rangle$, where $A = \{0, 1, a, b, c, d, e\}$ and the elements of S are arranged in the following order:

(1) $c1 \to 0ac$,
(2) $a0 \to 0a$,
(3) $ea \to ae$,
(4) $0a \to ae0$,
(5) $0c \to d$,
(6) $ed \to d1$,
(7) $ad \to d$,
(8) $0d \to d$,
(9) $bc \to \cdot 1$,
(10) $bd \to \cdot 1$,
(11) $1 \to bc$.

To illustrate the work of this algorithm we write the number 2:

$$\mathbf{111} \to b\mathbf{c1}1 \to b0a\mathbf{c1} \to b0\mathbf{a0}ac \to b0\mathbf{0a}ac \to b\mathbf{0a}e0ac \to$$
$$\to bae0e\mathbf{0a}c \to bae0\mathbf{ea}e0c \to bae\mathbf{0a}ee0c \to ba\mathbf{ea}e0ee0c \to$$
$$\to baaee0ee\mathbf{0c} \to baaee0e\mathbf{ed} \to baaee0\mathbf{ed}1 \to baaee\mathbf{0d}11 \to$$
$$\to baae\mathbf{ed}11 \to baa\mathbf{ed}111 \to ba\mathbf{ad}1111 \to b\mathbf{ad}1111 \to$$
$$\to \mathbf{bd}1111 \to \cdot 11111.$$

We proceed to describe the class of algorithms introduced by A. M. Turing and E. L. Post in 1936.

Let two finite sets A and Q be given containing no letters L and R. A set of quadruples $P = \{ \langle x_i, y_i, u_i, v_i \rangle \mid i \leqslant m \}$ is said to be a *program* with an exterior alphabet A and an interior alphabet Q if $x_i \in Q$, $y_i \in A$, $u_i \in Q$ and $v_i \in A \cup \{L, R\}$ for any $i \leqslant m$. In what follows the elements of a program $\langle x, y, u, v \rangle$ will be called instructions and denoted by $xy \to uv$.

DEFINITION. A *Turing machine* is a 6-tuple $\langle A, Q, a_0, q_0, q_1, P \rangle$ satisfying the following conditions:

(1) the sets A, Q are finite, do not intersect and do not contain the letters L, R;

(2) $a_0 \in A$; $q_0, q_1 \in Q$;

(3) P is a program with an exterior alphabet A and an iterior alphabet Q such that

(a) there are no two distinct quadruples in P in which the first and respectively second terms coincide.

(b) q_0 is not the first term in any of the quadruples of P.

A machine word with an exterior alphabet A and an interior alphabet Q (or simpply *a machine word in $\langle A, Q \rangle$*) is a word in the alphabet $A \cup Q$ such that α is a word in an alphabet $A \cup \{q\}$ for some $q \in Q$ and α contains exactly one occurrence of the symbol q.

Suppose α is a word in an alphabet B and $a \in B$. A word $a\alpha a$ will be denoted by α^a. If $\alpha = b\alpha_1 c$, where $b, c \in B$, then α_a will denote

(a) a word α_1 if $b = c = a$;

(b) a word $\alpha_1 c$ if $b = a$ and $c \neq a$;

(c) a word $b\alpha_1$ if $c = a$ and $b \neq a$;

(d) a word α if $b \neq a$ and $c \neq a$.

Let α and β be machine words in $\langle A, Q \rangle$ and let an element $q \in Q$ occur in α. We shall say that a Turing machine $M = \langle A, Q, a_0, q_0, q_1, P \rangle$ *converts a word α into a word β* (we write $\alpha \overset{M}{\rightarrow} \beta$) if the following three conditions hold:

(1) if $\alpha^{a_0} = \alpha_1 q a \alpha_2$ and $qa \to rb \in P$, $b \in A$, then $\beta = = (\alpha_1 r b \alpha_2)_{a_0}$;

(2) if $\alpha^{a_0} = \alpha_1 a q b \alpha_2$ and $qb \to rL \in P$, then $\beta = (\alpha_1 r a b \alpha_2)_{a_0}$;

(3) if $\alpha^{a_0} = \alpha_1 q a \alpha_2$ and $qa \to rR \in P$, then $\beta = (\alpha_1 a r \alpha_2)_{a_0}$.

Note that a machine M can convert a word α only into one word. This follows from condition 3(a) of the definition of a Turing machine. If a machine word α in $\langle A, Q \rangle$ is not converted by a Turing machine $M = \langle A, Q, a_0, q_0, q_1, P \rangle$ into any word β, it is said that α is a *no-go word for M.* Notice that condition 3(b) of the definition of a Turing machine implies that if a machine word α contains a symbol q_0, then it is a no-go word for M.

Let α be a machine word in an alphabet B. A word obtained from α by replacing all occurrences of a symbol b by the empty word is denoted by α / b.

DEFINITION. Let $M = \langle A, Q, a_0, q_0, q_1, P \rangle$ be a Turing machine and let α, β be words in an alphabet $A \setminus \{a_0\}$. We shall say that the machine *M transforms the word* α into the word β (we write $M(\alpha) = \beta$) if there is a sequence $\gamma_0, \ldots, \gamma_n$ of machine words in $\langle A, Q \rangle$ satisfying the following conditions:

(1) $\gamma_0 = q_1 \alpha$;

(2) $\beta = (\gamma_n / q_0) / a_0$;

(3) $\gamma_i \overset{M}{\to} \gamma_{i+1}, i < n$.

Notice that if conditions (1) to (3) hold for the sequence $\gamma_0, \ldots, \gamma_n$, then γ_n contains an occurrence of q_0 since β is a word in $A \setminus \{a_0\}$.

It is clear that the machine M can transform α only into one word. If M does not transform α into any word, then we shall say that M is not applicable to α or that the value of $M(\alpha)$ is not defined. In this case either there is an infinite sequence $\gamma_0, \ldots, \gamma_n, \ldots, n \in \omega$, for some $\gamma_0 = q_1 \alpha$ and $\gamma_i \overset{M}{\to} \gamma_{i+1}, i \in \omega$, or there is a finite sequence $\gamma_0, \ldots, \gamma_n$ satisfying conditions (1) and (3) and γ_n is a no-go word not containing q_0.

DEFINITION. A partial function $f: X \to \omega, X \subseteq \omega^n$, is said to be *Turing computable* if there is a Turing machine $M = \langle A, Q, a_0, q_0, q_1, P \rangle$ for which the following conditions hold:

(a) $0, 1 \in A, a_0 \neq 0, a_0 \neq 1$;

(b) M is applicable to the notation of an n-tuple $a \Leftrightarrow a \in X$;

(c) $M(\underset{\sim}{a}) = \underline{f(a)}$ for $a \in X$.

Such a machine will be called a *Turing machine computing the function f.*

It is obvious that all Turing computable partial functions are computable.

EXAMPLE 4. Construct a Turing machine M computing a function $f(n) = 2n$. Let $M = \langle A, Q, a, q_0, q_1, P\rangle$, where $A = \{0, 1, a\}$, $Q = \{q_0, q_1, q_2, q_3, q_4\}$ and P consists of the following quadruples:

$$\begin{array}{lll} q_1 1 \to q_3 0, & q_3 0 \to q_3 R, & q_3 1 \to q_2 0, \\ q_2 0 \to q_2 L, & q_2 a \to q_3 0, & q_3 a \to q_4 L, \\ q_4 0 \to q_4 1, & q_4 1 \to q_4 L, & q_4 a \to q_0 a. \end{array}$$

Let the reader see for himself that this machine does in fact compute the function $f(n) = 2n$. To illustrate its work we write out the "process of computing" $f(2)$:

$$\begin{aligned} & q_1 111 \xrightarrow{M} q_3 011 \xrightarrow{M} 0q_3 11 \xrightarrow{M} 0q_2 01 \xrightarrow{M} q_2 001 \xrightarrow{M} \\ & \xrightarrow{M} q_2 a001 \xrightarrow{M} q_3 0001 \xrightarrow{M} 0q_3 001 \xrightarrow{M} 00q_3 01 \xrightarrow{M} 000q_3 1 \xrightarrow{M} \\ & \xrightarrow{M} 000q_2 0 \xrightarrow{M} 00q_2 00 \xrightarrow{M} 0q_2 000 \xrightarrow{M} q_2 0000 \xrightarrow{M} q_2 a0000 \xrightarrow{M} \\ & \xrightarrow{M} q_3 00000 \xrightarrow{M} 0q_3 0000 \xrightarrow{M} 00q_3 000 \xrightarrow{M} 000q_3 00 \xrightarrow{M} \\ & \xrightarrow{M} 0000q_3 0 \xrightarrow{M} 00000q_3 \xrightarrow{M} 0000q_4 0 \xrightarrow{M} 0000q_4 1 \xrightarrow{M} \\ & \xrightarrow{M} 000q_4 01 \xrightarrow{M} 000q_4 11 \xrightarrow{M} 00q_4 011 \xrightarrow{M} 00q_4 111 \xrightarrow{M} \\ & \xrightarrow{M} 0q_4 0111 \xrightarrow{M} 0q_4 1111 \xrightarrow{M} q_4 01111 \xrightarrow{M} q_4 11111 \xrightarrow{M} \\ & \xrightarrow{M} q_4 a11111 \xrightarrow{M} q_0 a11111. \end{aligned}$$

The following theorem holds.

THEOREM 1. *The class of Turing-computable partial functions coincides with the class of normally computable partial functions.*

The proof that Turing-computable functions are normally computable will be left as an exercise to the reader. The proof of the other part of the theorem is rather cumbersome, consisting essentially of writing out a great number of programs, and so is omitted here.

By virtue of Theorem 1 the following thesis is equivalent to the normalization principle for partial functions: *any computable partial function is Turing-computable* (*Turing's thesis*).

Exercises

1. Construct a normal algorithm equivalent with respect to the alphabet $\{Q_0, Q_1, \wedge, \vee, \neg, \rightarrow, (,)\}$ to the algorithm of Example 1.

2. Construct a normal algorithm $\mathfrak{A}$ over an alphabet A such that for any word α in A $\mathfrak{A}(\alpha) = \alpha\alpha$.

3. Prove that the class of Turing computable functions is closed under a superposition.

36. RECURSIVE FUNCTIONS

This section presents a method for refining the concept of countable function, which may be called algebraic since the class of functions to be defined is generated from some elementary functions with the aid of some operations.

Recall that by a partial function we mean here any mapping $f: X \rightarrow \omega$, where $X \subseteq \omega^n$ for some $n \in \omega$. In this case n is called the number of places in a partial function f and denoted by $\nu(f)$. If $f: X \rightarrow \omega$ is a partial function, then f is said to be *nowhere defined* when $X = \varnothing$ and *completely defined* when $X = \omega^{\nu(f)}$*. In what follows the completely defined partial function is called simply a function. A partial function with a number of places n is an n-place partial function. The case $n = 0$ is possible. Then the 0-place function f: $\omega^0 \rightarrow \omega$ consists of a single pair $\langle \varnothing, n \rangle$ for some $n \in \omega$ and is often identified with the number n. Throughout the following the letters m, k, i and j, possibly with indices, denote natural numbers.

Let $f: X \rightarrow \omega$ be an n-place partial function. If $\langle m_1, \ldots, m_n \rangle \in \in X$, then $f(m_1, \ldots, m_n)$ is the value of f on an n-tuple $\langle m_1, \ldots \ldots, m_n \rangle$. If $\langle m_1, \ldots, m_n \rangle \notin X$, then we shall say that $f(m_1, \ldots \ldots, m_n)$ is not defined or that f is not defined on an n-tuple $\langle m_1, \ldots, m_n \rangle$.

It is clear that to define an n-place partial function f it suffices, for any n-tuple $\langle m_1, \ldots, m_n \rangle$, to say whether $f(m_1, \ldots, m_n)$ is defined and if it is, then to find the number $k = f(m_1, \ldots, m_n)$. If

---

* Note that if f is a partial function, then n is defined for f uniquely when f is not a nowhere defined function. Nowhere defined functions with numbers of places n and m for any $n, m \in \omega$ are equal.

f and g are partial functions, then we write

$$f(m_1, \dots, m_n) = g(m_1, \dots, m_n)$$

when both sides of the equation are defined and are equal or when both sides are not defined.

Let $\mathfrak{F}_n$ be the family of all n-place partial functions and let $\mathfrak{F} = \bigcup_{n \in \omega} \mathfrak{F}_n$ be the family of all partial functions.

We define on the family $\mathfrak{F}$ of all partial functions operators S, R, M which preserve the computability of functions.

Suppose $n, k \in \omega$, f is an $(n + 1)$-place partial function and $g_0, \dots, g_n$ are k-place partial functions. We define a k-place partial function h as follows: $h(m_1, \dots, m_k)$ is not defined if at least one of the partial functions $g_0, \dots, g_n$ is not defined on $\langle m_1, \dots, m_k \rangle$, and if all $g_0, \dots, g_n$ are defined on $\langle m_1, \dots, m_k \rangle$, then

$$h(m_1, \dots, m_k) = f(g_0(m_1, \dots, m_k), \dots, g_n(m_1, \dots, m_k)).$$

We shall say that h *is obtained by regular superposition from* f, $g_0, \dots, g_n$ and designate this as follows: $h = S^{k, n}(f, g_0, \dots, g_n)$. The operator (*of regular superposition*) $S^{k, n}$ is a completely defined mapping of $\mathfrak{F}_{n+1} \times \mathfrak{F}_k^{n+1}$ into $\mathfrak{F}_k$ and preserves computability, i. e. if partial functions $f \in \mathfrak{F}_{n+1}$; $g_0 \dots g_n \in \mathfrak{F}_k$ are computable, then so is the partial function $S^{k, n}(f, g_0, \dots, g_n)$. The superscripts of S will be omitted and as a rule we shall use the more customary but less precise notation $f(g_0, \dots, g_n)$ instead of $S(f, g_0, \dots, g_n)$.

Let $n \in \omega, f \in \mathfrak{F}_n, g \in \mathfrak{F}_{n+2}$. We define for f and g an $(n + 1)$-place partial function h so that for any $m_1, \dots, m_n \in \omega$

$$h(m_1, \dots, m_n, 0) = f(m_1, \dots, m_n);$$

$h(m_1, \dots, m_n, k + 1)$ is not defined if $h(m_1, \dots, m_n, k)$ is not defined and $h(m_1, \dots, m_n, m_n, k + 1) = g(m_1, \dots, m_n, k, h(m_1, \dots, m_n, k))$ if $h(m_1, \dots, m_n, k)$ is defined. It is obvious that h is uniquely defined for f and g and is computable if f and g are computable. This definition of h from f and g gives an operator $R^{n+1}: \mathfrak{F}_n \times \mathfrak{F}_{n+2} \rightarrow \mathfrak{F}_{n+1}$ called *primitive recursion operator*. The function $h = R^{n+1}(f, g)$ is said to *be obtained by primitive recursion from f and g*. The superscript of the operator R^{n+1} will be omitted.

Let $n \in \omega$, $f \in \mathfrak{F}_{n+1}$. We define for f an n-place partial function g such that for any $k, m_1, \dots, m_n \in \omega$ $g(m_1, \dots, m_n) = \cdot k$ if and only if $f(m_1, \dots, m_n, 0) = 0$ and $k = 0$ or $k > 0$ and $f(m_1, \dots$ $\dots, m_n, 0), \dots, f(m_1, \dots, m_n, k - 1)$ are defined and are not zero and $f(m_1, \dots, m_n, k) = 0$. It is clear that such a function g exists and is uniquely defined for f; moreover, if f is a computable function, then the computability of g is obvious from the definition of g. Thus we are given an operator M^n, the *minimization operator*, from $\mathfrak{F}_{n+1}$ into $\mathfrak{F}_n$; if $g = M^n(f)$, then we shall say that g *is obtained from f by minimization.*

Basis functions are o, s, I^n_m $(1 \leqslant m \leqslant n)$, where o is a one-place function assuming a value 0 on any n, s is a one-place function assuming a value $n + 1$ on a number n and I^n_m is an n-place function assuming a value k_m on a collection $\langle k_1, \dots, k_n \rangle$. It is obvious that the basis functions are computable.

DEFINITION. A partial function f is said to be *partially recursive* if there is a finite sequence of partial functions $g_0, \dots, g_k$ such that $g_k = f$ and every g_i, $i \leqslant k$, is either a basis function or is obtained from some previous functions by regular superposition, primitive recursion or minimization. The sequence $g_0, \dots, g_k$ is the *determining sequence for f*. If for a completely defined partially recursive function f there is a determining sequence consisting only of completely defined functions, then f is said to be *recursive*.

In the next section we shall prove that any completely defined partially recursive function is recursive.

It readily follows from this definition and the above remarks on the preservation of computability by the operators S, R, M that any partially recursive function is computable.

The converse statement is called *Church's thesis*:

Any computable partial function is partially recursive.

Historically it is this assertion that was the earliest precise mathematical definition of an (algorithmically) computable function.

We have the following theorem whose proof is omitted because of its being too cumbersome.

THEOREM 2. *The class of partially recursive functions coincides with the class of Turing computable functions.*

Thus Turing's thesis is equivalent to Church's.

Let $k, n \in \omega$, let α be some mapping of a set $\{1, \dots, k\}$ into a set $\{1, \dots, n\}$ and let f be a k-place partial function. An n-place partial function g is said to *be obtained from f by substituting α* if for any $m_1, \dots, m_n \in \omega$

$$g(m_1, \dots, m_n) = f(m_{\alpha 1}, \dots, m_{\alpha k}).$$

This will be denoted by $g = f^{\alpha}$.

PROPOSITION 1. *If f is a partially recursive function and g is obtained from f by substituting α, then g is partially recursive.*

PROOF. It is easy to verify that if $g = f^{\alpha}$, then

$$g = S^{n, k-1}(f, I^n_{\alpha 1}, \dots, I^n_{\alpha k}). \ \square$$

PROPOSITION 2. *The following functions are recursive*:

(1) *zero-place functions n, $n \in \omega$*;

(2) *the two-place addition function* $+$;

(3) *the two-place multiplication function* $\cdot$;

(4) *the two-place truncated-difference function* $\dot{-}$ *defined as follows*:

$$m \dot{-} n = \begin{cases} m - n & \textit{if} \quad n \leqslant m \\ 0 & \textit{otherwise}; \end{cases}$$

(5) *one-place functions sg and $\overline{sg}$ defined as follows*:

$$sg(n) = \begin{cases} 0 & \textit{if} \quad n = 0 \\ 1 & \textit{otherwise}; \end{cases}$$

$$\overline{sg}(n) = \begin{cases} 1 & \textit{if} \quad n = 0 \\ 0 & \textit{otherwise}; \end{cases}$$

(6) *the two-place identification function δ defined as follows*:

$$\delta(n, m) = \begin{cases} 0 & \textit{if} \quad n = m \\ 1 & \textit{otherwise}. \end{cases}$$

PROOF. We show that the zero-place function $\{\langle \varnothing, n \rangle\}$ is recursive by induction on n. The function $\{\langle \varnothing, 0 \rangle\}$ is equal to $M(o)$. If $\{\langle \varnothing, n \rangle\}$ is recursive, then the recursive function $s(\{\langle \varnothing, n \rangle\}) = \{\langle \varnothing, n + 1 \rangle\}$. Since $n + 0 = n$ and $n + (m + 1) = (n + m) + 1$, then the function $+$ equals $R(I^1_1, s(I^3_3))$. It follows from $n \cdot 0 = 0$ and $n \cdot (m + 1) = n \cdot m + n$ that the function $\cdot$ equals $R(0, I^3_1 + I^3_3)$.

To show that the truncated difference $\dot{-}$ is recursive, consider the one-place function $\dot{-}\,1$ defined as follows:

$$n \dot{-} 1 = \begin{cases} 0 & \textit{if} \quad n = 0 \\ n - 1 & \textit{if} \quad n \neq 0. \end{cases}$$

It equals $R(0, I_1^2)$ and is therefore recursive. Since $n \dot{-} (m + 1) = = (n \dot{-} m) \dot{-} 1$, the function $\dot{-}$ equals $R(I_1^1, I_3^3 \dot{-} 1)$ and hence is also recursive.

The recursiveness of functions (5) follows from the equations $\mathrm{sg} = R(0, s(o(I_1^2)))$ and $\overline{\mathrm{sg}} = R(1, o(I_1^2))$.

Let α: $\{1, 2\} \to \{1, 2\}$ be such that $\alpha(1) = 2$, $\alpha(2) = 1$ and let f be a function obtained from the function $\dot{-}$ by substituting α. Then for the function δ the equation $\delta = S\,(\mathrm{sg}, S(+, \dot{-}, f))$ is true. It follows from the recursiveness of the functions sg, $\dot{-}$ and Proposition 1 that the identification function δ is recursive. ☐

To define recursive functions and study their properties it is convenient to use a special formal language R_Σ similar to that described in Sec. 16. Let $V = \{v_i \,|\, i \in \omega\}$ be a set of variables whose elements are denoted by x, y, z, w, and u possibly with indices.

Suppose $\Sigma = (R, F, \mu)$ is some finite signature such that $F \supseteq \supseteq F_0 = \{0, s, +, \cdot\}$, where 0 is the symbol of a zero-place function, s is the symbol of a one-place function, $+$ and $\cdot$ are the symbols of two-place functions; $R \supseteq R_0 = \{<\}$, where $<$ is the symbol of a two-place predicate.

Defining the expressions (the syntax) of the language R_Σ will also depend on the semantics of this language. Therefore the syntax and semantics will be defined simultaneously; but first assume a fixed algebraic system Ω_Σ of a signature Σ with basic set ω and such that the values of the symbols of $\Sigma_0 = (R_0, F_0, \mu_0)$ coincide with the functions and the predicate denoted by these symbols earlier (for example, to the symbol $\cdot$ there corresponds the operation of multiplication of natural numbers).

So by simultaneous induction we shall define the notion of *Σ-term*, of *Σ-formula* (it would be more precise to speak of Ω_Σ-terms and Ω_Σ-formulas), sets of free variables $FV(t)$ $(FV(\varphi))$ of a Σ-term t of a Σ-formula φ, a natural number $t[\eta]$ and a truth value $\varphi[\eta] \in \{T, F\}$ for any interpretation $\eta: X \to \omega$, where $X \subseteq V$, $FV(t) \subseteq X$, $FV(\varphi) \subseteq X$:

(a) the symbol 0 is a Σ-term, $FV(0) = \varnothing$ and $0[\eta] = 0$;

(b) a variable $x \in V$ is a Σ-term, $FV(x) = \{x\}$, $x[\eta] = \eta(x)$;

(c) if $f \in F$ is an n-place function symbol, $t_1, \ldots, t_n$ are Σ-terms, then $f(t_1, \ldots, t_n)$ are Σ-terms; $FV(f(t_1, \ldots, t_n)) = FV(t_1) \cup \ldots \cup FV(t_n)$; $f(t_1, \ldots, t_n)[\eta] = f^{\Omega_\Sigma}(t_1[\eta], \ldots, t_n[\eta])$, where f^{Ω_Σ} is an n-place operation of Ω_Σ corresponding to a signature symbol f;

(d) if Q is an n-place predicate symbol in R and $t_1, \ldots, t_n$ are Σ-terms, then $Q(t_1, \ldots, t_n)$ is a Σ-formula, $FV(Q(t_1, \ldots, t_n)) = FV(t_1) \cup \ldots \cup FV(t_n)$; $Q(t_1, \ldots, t_n)[\eta] = u \Leftrightarrow \langle t_1[\eta], \ldots, t_n[\eta]\rangle \in Q^{\Omega_\Sigma}$, where Q^{Ω_Σ} is an n-place predicate corresponding in Ω_Σ to a predicate symbol Q;

(e) if t_1, t_2 are Σ-terms, then $t_1 \approx t_2$ is a Σ-formula, $FV(t_1 \approx t_2) = FV(t_1) \cup FV(t_2)$, $(t_1 \approx t_2)[\eta] = u \Leftrightarrow t_1[\eta] = t_2[\eta]$;

(f) if φ and ψ are Σ-formulas, then $\neg\varphi$, $(\varphi\tau\psi)$ for $\tau \in \{\wedge, \vee, \to\}$ are also Σ-formulas, $FV(\neg\varphi) = FV(\varphi)$, $FV(\varphi\tau\psi) = FV(\varphi) \cup FV(\psi)$ and $(\neg\varphi)[\eta] = \neg(\varphi[\eta])$, $(\varphi\tau\psi)[\eta] = \varphi[\eta]\tau\psi[\eta]$, where $\neg, \wedge, \vee, \to$ are defined on the set $\{T, F\}$ by table (1) of Sec. 6, with "0" replaced by "F" and "1" replaced by "T";

(g) if φ is a Σ-formula, $x \in V$ and for any interpretation $\eta_1 : X \to \omega$ for which $x \notin X$ and $FV(\varphi) \subseteq X \cup \{x\}$ there is $n \in \omega$ such that $\varphi[\eta] = T$ for $\eta = \eta_1 \cup \{\langle x, n\rangle\}$, then $\mu x\varphi$ is a Σ-term, $FV(\mu x\varphi) = FV(\varphi) \setminus \{x\}$ and $(\mu x\varphi)[\eta]$ is the least $n_0 \in \omega$ for which $\varphi[\eta'] = T$, where $\eta' = (\eta \setminus \{\langle x, \eta x\rangle\}) \cup \{\langle x, n_0\rangle\}$.

It is easily established by induction on the construction of a Σ-term (of a Σ-formula) Θ that *for any interpretations* $\eta_0 : X_0 \to \omega$, $\eta_1 : X_1 \to \omega$ *such that* $FV(\Theta) \subseteq X_0 \cap X_1$ *and for all* $x \in FV(\Theta)$ $\eta_0(x) = \eta_1(x)$ *we have* $\Theta[\eta_0] = \Theta[\eta_1]$.

As usual we shall write $(t_1 + t_2)((t_1 \cdot t_2))$ instead of $+(t_1, t_2)(\cdot(t_1, t_2))$ and $(t_1 < t_2)$ instead of $<(t_1, t_2)$. In addition we shall use the usual abbreviations for terms and formulas accepted in arithmetic and the propositional calculus (for example, instead of $(x + ((z \cdot z) + (x \cdot y)))$ and $((\varphi \wedge \psi) \to \varphi)$ we shall write respectively $x + z^2 + xy$ and $((\varphi \wedge \psi) \to \varphi)$.

For a Σ-formula φ and an interpretation $\eta: X \to \omega$, $FV(\varphi) \subseteq X$, we shall often write "$\varphi[\eta]$ is true" or simply "$\varphi[\eta]$" instead of "$\varphi[\eta] = T$" and "$\varphi[\eta]$ is false" or "$\neg\varphi[\eta]$" instead of "$\varphi[\eta] = F$".

Let Θ be a Σ-term or a Σ-formula. An occurrence of x in Θ is said to be *free* if it is not in a subword of the form $\mu x\varphi$ which is a term. If the occurrence of a variable in Θ is not free it is said to be *bound*. It is easy to verify that the set $FV(\Theta)$ consists precisely of variables with free occurrences in Θ.

Suppose Θ is a Σ-term (a Σ-formula), $x_1, \ldots, x_n \in V$ are distinct variables, $t_1, \ldots, t_n$ are Σ-terms such that for any $i \in \{1, \ldots, n\}$ and any $x_i \in FV(t_i)$ no free occurrence in Θ of a variable y is contained in a term of the form $\mu y\varphi$ which is a subword of Θ. Then $(\Theta)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ denotes the result of replacing all free occurrences of variables $x_1, \ldots, x_n$ by Σ-terms $t_1, \ldots, t_n$ respectively.

By induction on the construction of a Σ-term and a Σ-formula it is easy to establish the following

PROPOSITION 3. *If Θ is a Σ-term (a Σ-formula), $x_1, \ldots, x_n \in V$ are distinct variables, $t_1, \ldots, t_n$ are Σ-terms such that for $\Theta, x_1, \ldots, x_n, t_1, \ldots, t_n$ the above conditions hold, then*

(1) $\Theta_1 = (\Theta)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ *is a Σ-term* (a *Σ-formula*), $FV(\Theta_1) \subseteq \subseteq (FV(\Theta) \setminus \{x_1, \ldots, x_n\}) \cup FV(t_1) \cup \ldots \cup FV(t_n)$;

(2) *for any interpretation $\eta: X \to \omega$ such that $(FV(\Theta) \setminus \{x_1, \ldots, x_n\}) \cup FV(t_1) \cup \ldots \cup FV(t_n) \subseteq X$ we have $\Theta_1[\eta] = \Theta[\eta']$, where $\eta' = \{\langle y, \eta(y)\rangle \mid y \in FV(\Theta), y \notin \{x_1, \ldots, x_n\}\} \cup \{\langle x_i, t_i[\eta]\rangle \mid i = 1, \ldots, n\}$.* □

A Σ-term (a Σ-formula) $\Theta_1 = (\Theta)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ is said to be obtained from Θ *by substituting* Σ-terms $t_1, \ldots, t_n$ for the variables $x_1, \ldots, x_n$.

Unfortunately, the conditions for Σ-terms to be substituted for variables do not always hold. To be always able to substitute we introduce the following notions. A Σ-term (a Σ-formula) Θ is said to be obtained from a Σ-term (a Σ-formula) Θ_1 *by replacing a bound variable* if Θ is obtained from Θ_1 by replacing the occurrence of a Σ-term $\mu x\varphi$ by $\mu y(\varphi)^x_y$, where $y \notin FV(\varphi)$. Σ-terms (Σ-formulas) Θ and Θ' are said to be *congruent* if there is a sequence $\Theta_1, \ldots, \Theta_n$ such that $\Theta_0 = \Theta$, $\Theta_n = \Theta'$ and Θ_{i+1}, $i > n$, is obtained from Θ_i by replacing a bound variable.

It is obvious that the congruent relation is an equivalence on a set of Σ-terms and Σ-formulas.

PROPOSITION 4. *If* Θ *and* Θ' *are congruent* Σ*-terms or* Σ*-formulas, then* $FV(\Theta) = FV(\Theta')$ *and for any interpretation* $\eta : FV(\Theta) \to \omega$ *we have* $\Theta[\eta] = \Theta'[\eta]$.

PROOF. It is easy to show by induction on the length of Θ that if Θ' is obtained from Θ by replacing a bound variable, then the statement of the proposition is true. We then proceed by induction on the length of the sequence $\Theta_0, \ldots, \Theta_n$ of the preceding definition. □

Note that for any Σ-term (Σ-formula) Θ, any collection of pairwise distinct variables $x_1, \ldots, x_n$ and any Σ-terms $t_1, \ldots, t_n$ there is a Σ-term (a Σ-formula) Θ' such that Θ' is congruent to Θ and satisfies the conditions for the substitution $(\Theta')^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$. Using this property and Proposition 4 we shall henceforth employ the notation $(\Theta)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ without caring about satisfying the conditions on bound variables, assuming that if these conditions do not hold, then $(\Theta)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ is $(\Theta')^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ for a Σ-term (a Σ-formula) congruent to Θ, with all conditions for the substitution already satisfied for Θ'.

Recall that a subset $X \subseteq A^n$ is called an n-place predicate on A. In what follows by predicates we mean predicates on ω. If X is an n-place predicate, then an n-place function π_X defined as follows: for any $m_1, \ldots, m_n \in \omega$

$$\pi_X(m_1, \ldots, m_n) = \begin{cases} 0 & \text{if } \langle m_1, \ldots, m_n \rangle \in X \\ 1 & \text{otherwise,} \end{cases}$$

is said to be a *representing* function for X.

Besides the representing function π_X of the predicate X one often uses the *characteristic* function χ_X of X which is related to π_X by the equation $\chi_X = \overline{\mathrm{sg}}\,(\pi_X)$.

A predicate X is said to be *recursive* if its representing function π_X is recursive.

An algebraic system Ω_Σ is said to be recursive if all functions and predicates corresponding to the symbols of Σ are recursive.

In what follows, speaking of Σ-formulas and Σ-terms (whose definition depends on a fixed algebraic system Ω_Σ) *we shall always assume that Ω_Σ is a recursive algebraic system.*

Notice that the predicates $\approx$, $<$ are recursive, since the representing function for $\approx$ is the identification function δ and the representing function for $<$ is the recursive function $\mathrm{sg}(s(I_1^2) \dot{-} I_2^2)$.

It is possible to associate with every Σ-term (Σ-formula) a family of functions (of predicates) which are *realized* by that Σ-term (by that Σ-formula). To denote these functions (predicates) we shall use an extension of R_Σ, adding another pair of symbols, the square brackets [,].

We proceed to precise definitions.

If t is a Σ-term and $FV(t) \subseteq \{x_1, \ldots, x_n\} \subseteq V$, $x_i \neq x_j$, for $i \neq j$ then $t[x_1, \ldots, x_n]$ will denote an n-place function assuming on an n-tuple $\langle m_1, \ldots, m_n \rangle \in \omega^n$ a value $t[\eta]$, where $\eta = \{\langle x_i, m_i \rangle \mid i = 1, \ldots, n\}$. If φ is a Σ-formula and $FV(\varphi) \subseteq \{x_1, \ldots, x_n\} \subseteq V$, $x_i \neq x_j$ for $i \neq j$, then $\varphi[x_1, \ldots, x_n]$ will denote a predicate $\{\langle m_1, \ldots, m_n \rangle \mid \varphi[\eta] = T$ for $\eta = \{\langle x_i, m_i \rangle \mid i = 1, \ldots, n\}\}$.

Notice that the same Σ-term t realizes many functions; for example, if $FV(t) \subseteq \{x, y\}$, then $t[x, y]$, $t[y, x]$ and $t[x, y, z]$ are in general different functions. The symbol $[x_1, \ldots, x_n]$ plays a role similar to that of quantifiers, it *relates* the variables $x_1, \ldots, x_n$; thus if $FV(t) \subseteq \{x_1, \ldots, x_n\}$ and $y_1, \ldots, y_n$ are pairwise distinct variables, then we have

$$t[x_1, \ldots, x_n] = (t)^{x_1, \ldots, x_n}_{y_1, \ldots, y_n}[y_1, \ldots, y_n].$$

PROPOSITION 5. *Any function and any predicate realized by a Σ-term and a Σ-formula respectively are recursive.*

PROOF. Let Θ be a Σ-term or a Σ-formula and let $FV(\Theta) \subseteq \{x_1, \ldots, x_k\}$; by induction on the construction of Θ we shall prove that $\Theta[x_1, \ldots, x_k]$ is recursive.

(a) If $\Theta = 0$, then $\Theta[x_1, \ldots, x_k] = M(o(I_1^k))$.

(b) If $\Theta = x \in V$, then $x = x_{i_0}$ for some $i_0 \in \{1, \ldots, k\}$; so $\Theta[x_1, \ldots, x_k] = I_{i_0}^k$.

(c) Let $\Theta = f(t_1, \ldots, t_n)$, where f is an n-place function symbol, $t_1, \ldots, t_n$ are Σ-terms; we have $FV(\Theta) = FV(t_1) \cup \ldots \cup$

$\cup\ FV(t_n) \subseteq \{x_1, \ldots, x_k\}$; by the induction hypothesis k-place functions $g_1 = t_1[x_1, \ldots, x_k], \ldots, g_n = t_n[x_1, \ldots, x_k]$ are recursive. If f^{Ω_Σ} is an n-place recursive function corresponding in a model Ω_Σ to the function symbol f, then obviously $\Theta[x_1, \ldots, x_n] = S(f^{\Omega_\Sigma}, g_1, \ldots, g_n) = f^{\Omega_\Sigma}(g_1, \ldots, g_n)$.

(d) Let $\Theta = Q(t_1, \ldots, t_n)$, where Q is an n-place predicate symbol and $t_1, \ldots, t_n$ are Σ-terms. We have $FV(\Theta) = FV(t_1) \cup \ldots \cup FV(t_n) \subseteq \{x_1, \ldots, x_k\}$; by the induction hypothesis k-place functions $g_1 = t_1[x_1, \ldots, x_k], \ldots, g_n = t_n[x_1, \ldots, x_k]$ are recursive. If Q^{Ω_Σ} is an n-place predicate corresponding in Ω_Σ to the predicate symbol Q, then according to our convention Q^{Ω_Σ} is a recursive predicate; therefore π_Q, the representing function of Q^{Ω_Σ}, is recursive. It is easy to verify that the k-place recursive function $S(\pi_Q, g_1, \ldots, g_n)$ is the representing function for the predicate $\Theta[x_1, \ldots, x_k]$; hence this predicate is recursive.

(e) Let $\Theta = t_1 \approx t_2$, where t_1, t_2 are Σ-terms; the representing function for the predicate $\Theta[x_1, \ldots, x_k]$ is a recursive function $S(\delta, t_1[x_1, \ldots, x_k], t_2[x_1, \ldots, x_k])$.

(f) The case where Θ is of the form $\neg\varphi$ or $(\varphi\tau\psi)$ for $\tau \in \{\wedge, \vee, \rightarrow\}$ and for Σ-formulas φ and ψ is quite obvious and will be left to the reader.

(g) Let $\Theta = \mu x\varphi$, where φ is a Σ-formula and conditions (g) of the definition of Σ-terms and Σ-formulas hold. Then $FV(\varphi) \subseteq \subseteq \{x_1, \ldots, x_k, x\}$. It is assumed that x is distinct from all the variables $x_1, \ldots, x_k$; if this is not the case, then we choose $y \in V$ to be distinct from $x_1, \ldots, x_k$ and to have no occurrences in φ and consider a Σ-term $\Theta' = \mu y(\varphi)^x_y$ instead of Θ. By the induction hypothesis it may be assumed that the $(k + 1)$-place function g representing the predicate $\varphi[x_1, \ldots, x_k, x]$ is recursive. Then it is easy to see that $\Theta[x_1, \ldots, x_k] = M(g)$. Hence $\Theta[x_1, \ldots, x^1]$ is recursive. □

Our main task in the remainder of this section is to prove that *any recursive function and any recursive predicate is realized by a* Σ_0*-term and a* Σ_0*-formula*. Such terms and formulas will be called *recursive*.

An important step in the proof of this statement is to consider the following situation: a signature Σ' is obtained from Σ by adding one k-place function symbol f; an algebraic system Ω_Σ is a restriction of an algebraic system $\Omega_{\Sigma'}$. Notice that in this case any Σ-term is simultaneously a Σ'-term.

PROPOSITION 6. *If there is a Σ-term t_0 such that a function $f^{\Omega_{\Sigma'}}$ corresponding in $\Omega_{\Sigma'}$ to the symbol f is realized by a term t_0, then from any Σ'-term t' and any Σ'-formula φ' we can effectively construct a Σ-term t and a Σ-formula φ such that $FV(t) = FV(t')$, $FV(\varphi) = FV(\varphi')$ and for any interpretation $\eta \colon X \to \omega$, $FV(t) \subseteq X (FV(\varphi) \subseteq X)$ we have $t'[\eta] = t[\eta]$ or $\varphi'[\eta] = \varphi[\eta]$ respectively.*

PROOF. Let $f^{\Omega_{\Sigma'}} = t_0[x_1, \dots, x_k]$. For any Σ'-term (any Σ'-formula) Θ we define inductively a word $r(\Theta)$ as follows: (a) if Θ does not contain the symbol f, i. e. if Θ is a Σ-term or a Σ-formula, then $r(\Theta) = \Theta$;

(b) if $g \in F'$ is an n-place function symbol distinct from f and $t_1, \dots, t_n$ are Σ'-terms, then $r(g(t_1, \dots, t_n)) = g(r(t_1), \dots, r(t_n))$;

(c) if $t_1, \dots, t_k$ are Σ'-terms, then $r(f(t_1, \dots, t_k)) = (t_0)^{x_1, \dots, x_k}_{r(t_1), \dots, r(t_k)}$;

(d) if Q is an n-place predicate symbol of $R' = R$, $t_1, \dots, t_n$ are Σ'-terms, then $r(Q(t_1, \dots, t_n)) = Q(r(t_1), \dots, r(t_n))$;

(e) $r(t_1 \approx t_2) = (r(t_1) \approx r(t_2))$ if t_1, t_2 are Σ'-terms;

(f) $r(\neg \varphi) = \neg r(\varphi)$, $r(\varphi \tau \psi) = (r(\varphi) \tau r(\psi))$ for $\tau \in \{\wedge, \vee, \to\}$ if φ, ψ are Σ'-formulas;

(g) $r(\mu x \varphi) = \mu x r(\varphi)$ for a Σ'-formula φ.

By induction on the construction of Σ'-terms and Σ'-formulas, using Propositions 3 and 4 and the definition of Σ-terms it is not hard to prove simultaneously the following statements:

(1) *for any Σ'-term t $r(t)$ is a Σ-term and $FV(t) = FV(r(t))$;*

(2) *for any Σ'-formula φ $r(\varphi)$* is a Σ-formula and $FV(\varphi) = FV(r(\varphi))$;

(3) if Θ *is a Σ'-term or a Σ-formula*, $FV(\Theta) \subseteq X$, $\eta \colon X \to \omega$ *is an interpretation*, *then* $\Theta[\eta] = r(\Theta)[\eta]$.

It is clear that these statements imply the conclusion of the proposition as well. □

It is proved quite similarly that a predicate symbol of a signature can be eliminated from $R' \setminus R$ when there is a Σ-formula without that predicate symbol that realizes the corresponding predicate in an algebraic system $\Omega_{\Sigma'}$. We shall therefore refer to Proposition 6 for the case of a predicate too.

If a Σ-formula φ is given, then $\mu x \varphi$ is not always a Σ-term, and Σ-formulas with quantifiers $\exists x \varphi$ and $\forall x \varphi$ were never assumed by us. It is, therefore, convenient to use at least "limited" analogues of these operators.

DEFINITION. Let φ be a Σ-formula, t be a Σ-term, $x \in V$ and $x \notin FV(t)$. We introduce the following notation:

(a) $\mu x \leqslant t \varphi = \mu x(\varphi \vee x \approx s(t))$;

(b) $\exists x \leqslant t \varphi = (\mu x \leqslant t \varphi) < s(t)$:

(c) $\forall x \leqslant t \varphi = \neg \exists x \leqslant t \neg \varphi$.

It is obvious that $\mu x = t\varphi$, $\exists x \leqslant t\varphi$ and $\forall x = t\varphi$ are a Σ-term and Σ-formulas, $FV(\mu x \leqslant t\varphi) = FV(\exists x \leqslant t\varphi) = FV(\forall x \leqslant t\varphi) = (FV(\varphi) \cup FV(t)) \setminus \{x\}$, and for an interpretation $\eta\colon (FV(t) \cup FV(\varphi)) \setminus \{x\} \to \omega$ we have

$$(\mu x \leqslant t\varphi)[\eta] = \begin{cases} \text{the least } n \leqslant t[\eta] \text{ for which} \\ \varphi[\eta'], \text{ where } \eta' = \eta \cup \{\langle x, n\rangle\}, \\ \text{if there is such an } n \\ t[\eta] + 1 \text{ otherwise;} \end{cases}$$

$$(\exists x \leqslant t\varphi)[\eta] = T \Leftrightarrow (\text{there is } n \leqslant t[\eta] \text{ for which } \varphi[\eta'] = T, \text{ where } \eta' = \eta \cup \{\langle x, n\rangle\});$$

$$(\forall x \leqslant t\varphi)[\eta] = T \Leftrightarrow (\text{for all } n \leqslant t[\eta] \text{ we have } \varphi[\eta'] = T, \text{ where } \eta' = \eta \cup \{\langle x, n\rangle\}).$$

We introduce a number of recursive functions and predicates, adding corresponding symbols to Σ_0. We add to Σ_0 the symbols for the functions defined in Proposition 2 and not contained in Σ_0:

(1) the two-place function symbol $\dot{-}$ coinciding with the notation of the corresponding function on ω;

(2) the two one-place function symbols sg and $\overline{\text{sg}}$;

(3) the two-place function symbol δ.

In addition we shall use the abbreviation n for the Σ_0-term $s(\ldots s(0)\ldots)$, where s occurs n times, $n \in \omega$.

An algebraic system Ω_Σ of the signature obtained is defined in a natural way. Notice that each symbol we have introduced satisfies the conditions of Proposition 6:

(1) $\dot{-} = \mu z((z \approx 0 \wedge (y \approx x \vee x < y)) \vee (y < x \wedge y + z \approx x))[x, y]$;
(2) $\overline{\mathrm{sg}} = (1 \dot{-} x)[x]$; $\mathrm{sg} = (1 \dot{-} \overline{\mathrm{sg}}(x))[x]$;
(3) $\delta = \mu z((x \approx y \wedge z \approx 0) \vee (\neg x \approx y \wedge \neg z \approx 0))[x, y]$.

Notice that on the right-hand sides of these relations new function symbols are also used for which a term expression has already been given. We introduce yet some more recursive functions and a recursive predicate, and the corresponding symbols, important for our further purposes:

(4) $\leqslant$ is a two-place predicate having its usual meaning on ω; the signature symbol will coincide with this notation;

(5) a two-place function $[/]$ realized by a term as follows:

$$[/] = \mu z((x < (s(z) \cdot y)) \vee (y \approx 0 \wedge z \approx x))[x, y],$$

the signature symbol will be the same; instead of writing $[/]\,(m, n)$ we shall write $[m/n]$; the term $[/](t_1, t_2)$ will also be written as $[t_1/t_2]$;

(6) a one-place function $[\sqrt{\ }]$ realized by a term as follows

$$[\sqrt{\ }] = \mu y(x < s(y)^2)[x],$$

the signature symbol being the same; instead of $[\sqrt{\ }](n)$ we write $[\sqrt{n}]$ and instead of $[\sqrt{\ }](t)$ we write $[\sqrt{t}]$;

(7) a two-place rest function realized by a term as follows:

$$\mathrm{rest} = (x \dot{-} ([x/y] \cdot y))[x, y],$$

rest being the corresponding signature symbol;

(8) a two-place c function realized by a term as follows:

$$c = [((x + y)^2 + 3x + y)/2][x, y],$$

c being the corresponding signature symbol;

(9) a one-place function l realized by a term as follows:

$$l = (x \dot{-} [(([\sqrt{8x + 1}\ + 1)/2]) \times \times ([([\sqrt{8x + 1}] \dot{-} 1)/2])/2])[x],$$

l being the corresponding signature symbol;

(10) a one-place function r realized by a term as follows

$$r = ([([\sqrt{8x + 1}] \dot{-} 1)/2] \dot{-} l(x))[x],$$

r being the corresponding signature symbol;

(11) a two-place function β defined by a term as follows:

$$\beta = \mu z \leqslant r(x)(\exists w \leqslant l(x)((1 + (c(z, y) + 1)\cdot r(x))\cdot w = = l(x)))[x, y],$$

β being the corresponding signature symbol.

We denote by Σ_1 a signature (R_1, F_1, μ_1), where $F_1 = \{0, s, +, \cdot, \dot{-}, \mathrm{sg}, \overline{\mathrm{sg}}, \delta, [/], [\sqrt{\ }], \mathrm{rest}, c, l, r, \beta\}$ and $R_1 = \{<, \leqslant\}$.

Using Proposition 6, it is easy to show that *from any* Σ_1*-formula* φ_1 *and any* Σ_1*-term* t_1 *we can effectively construct a recursive formula* φ_0 *and a recursive term* t_0 *such that* $FV(\varphi_0) = FV(\varphi_1)$, $FV(t_0) = FV(t_1)$ *and if* $FV(\varphi_0) \subseteq \{x_1, \ldots, x_n\}(FV(t_0) \subseteq \{x_1, \ldots, x_n\})$, *then* $\varphi_0[x_1, \ldots, x_n] = \varphi_1[x_1, \ldots, x_n]$ *and* $t_0[x_1, \ldots, x_n] = [t_1[x_1, \ldots, x_n]$ *respectively.*

Now note some properties of the functions introduced above.

For any $m, n \in \omega$, $[m/n]$ *is the integral part of the fraction* $\frac{m}{n}$ *if* $n \neq 0$ *and* $[m/n] = m$ *if* $n = 0$.

For any $m, n \in \omega$, $\mathrm{rest}(m, n)$ *is the remainder of a division of* m *by* n *if* $n \neq 0$; $\mathrm{rest}(m, n) = m$ *if* $n = 0$.

For any $m \in \omega$ $[\sqrt{m}]$ *is the integral part of the square root of* m.

We consider the functions c, l, r together.

PROPOSITION 7. *For the functions* c, l, r *and any* $m, n \in \omega$ *the following equations hold*:

(1) $c(l(n), r(n)) = n$;
(2) $l(c(m, n)) = m$;
(3) $r(c(m, n)) = n$.

In particular, c *maps* ω^2 *onto* ω *in a one-to-one manner.*

PROOF. The usual arithmetic notation will be used below to compute c, l, and r.

It follows from the equation $c(n, m) = \frac{(n + m)^2 + 3n + m}{2}$ that

$$8c(n, m) = 4(n + m)^2 + 12n + 4m.$$

The right-hand side of this equation permits the following two representations: $(2n + 2m + 1)^2 + 8n - 1$ and $(2n + 2m + 3)^2 - 8m - 9$. Hence we obtain the relations:

$$(2n + 2m + 1)^2 \leqslant 8c(n, m) + 1 < (2n + 2m + 3)^2,$$

$$2n + 2m + 1 \leqslant [\sqrt{8c(n, m) + 1}] < 2n + 2m + 3,$$

$$2n + 2m + 2 \leqslant [\sqrt{8c(n, m) + 1}] + 1 < 2n + 2m + 4,$$

$$n + m + 1 \leqslant \left[\frac{[\sqrt{8c(n, m) + 1}] + 1}{2}\right] < n + m + 2.$$

Therefore

$$n + m + 1 = \left[\frac{[\sqrt{8c(n, m) + 1}] + 1}{2}\right],$$

$$n + m = \left[\frac{[\sqrt{8c(n, m) + 1}] + 1}{2}\right] \dot{-} 1 = \left[\frac{[\sqrt{8c(n, m) + 1}] \dot{-} 1}{2}\right].$$

Since

$$c(n, m) = \frac{(n + m)^2 + 3n + m}{2} = \frac{(n + m)(n + m + 1)}{2} + n,$$

we have

$$n = c(n, m) \dot{-} \frac{1}{2}\left[\frac{[\sqrt{8c(n, m) + 1}] + 1}{2}\right] \times \left[\frac{[\sqrt{8c(n, m) + 1}] \dot{-} 1}{2}\right],$$

$$m = \left[\frac{[\sqrt{8c(n, m) + 1}] \dot{-} 1}{2}\right] \dot{-} n.$$

Hence we get $l(c(n, m)) = n$, $r(c(n, m)) = m$.

If $n = c(i, j)$ for some $i, j \in \omega$, then from $l(c(i, j)) = i$ and $r(c(i, j)) = j$ we get $c(l(n), r(n)) = n$. Hence to prove the equation $c(l(n), r(n)) = n$ for any $n \in \omega$ it suffices to show that for any $n \in \omega$ there are $i, j \in \omega$ for which $n = c(i, j)$. From the definition of c we get $c(0, 0) = 0$. If $c(i, j) = m$ and $j > 0$, then it is easy to verify that $c(i + 1, j - 1) = m + 1$. If $c(i, j) = m$ and $j = 0$, then $c(0, i + 1) = m + 1$. □

We now turn to the (technically) very important function β.

PROPOSITION 8. *For any* $k \in \omega$ *and any* $n_0, \ldots, n_k \in \omega$ *there is a number* $m \in \omega$ *such that*

$$\beta(m, i) = n_i \qquad \textit{for all} \qquad i \leqslant k.$$

PROOF. Suppose $c = \max\{c(n_i, i) + 1 \mid i \leqslant k\}$ and $a = c!$. We show that for $0 \leqslant j < l \leqslant c$ the numbers $1 + ja$ and $1 + la$ are coprime. Suppose the contrary and let a prime number p divide $1 + ja$ and $1 + la$. Then p divides their difference $(1 + la) - (1 + ja) = (l - j)a$; then p divides $l - j$ or a, but since $l - j \leqslant c$, $l - j$ divides $a = c!$, so that in any case p divides a. But then $a = pa'$ and $1 + ja = (ja')p + 1$, and this number cannot be divided by p, a contradiction.

Suppose $s = (1 + (c(n_0, 0) + 1)a) \cdot (1 + (c(n_1, 1) + 1)a) \cdot \ldots \cdot (1 + (c(n_k, k) + 1)a) = \prod_{i \leqslant k} (1 + (c(n_i, i) + 1) \cdot a)$ and $m = c(s, a)$.

We show that it is this m that satisfies the conclusion of the proposition. Let $i \leqslant k$. Then $(1 + (c(n_i, i) + 1)a)$ divides $s(a = r(m), s = l(m))$. Suppose that for some $z \leqslant n_i$ $(1 + (c(z, i) + 1)a)$ also divides s. Since $z \leqslant n_i$, we have $c(z, i) \leqslant c(n_i, i) < c$. From this and from the above fact that numbers of the form $1 + ja$ and $1 + la, j \neq l \leqslant c$, are coprime it follows that $c(z, I) + 1$ must coincide with some $c(n_j, j) + 1, j \leqslant k$. But if $c(z, i) + 1 = c(n_j, j) + 1$, then $c(z, i) = c(n_j, j), i = j$ and $z = n_i$. Thus n_i is the least z such that $(1 + (c(z, i) + 1)a)$ divides s and $n_i \leqslant c(n_i, i) < c(n_i, i) + 1 \leqslant c \leqslant a = c! = r(m)$ and therefore $\beta(m, i) = n_i$. □

In what follows Σ_0-terms and Σ_0-formulas will be called recursive terms and formulas. The following theorem provides the characterization of recursive functions that was pointed out earlier.

THEOREM 3. *For a function f: $\omega^n \rightarrow \omega$ to be recursive it is necessary and sufficient that f be realized by some recursive term t_f.*

PROOF. Sufficiency was established earlier (Proposition 5). To prove necessity we proceed by induction on the minimum length of the determining sequence of recursive functions for f. In view of the foregoing it is only necessary to prove the existence of Σ_1-terms that realize functions. The basis functions o, s and I^n_m are realized by the Σ_0-terms $\mu y\ (x \approx x)$, $s(x)$ and x_m as follows:

$$o = \mu y(x \approx x)[x], \quad s = s(x)[x], \quad I^n_m = x_m[x_1, \ldots, x_n].$$

Suppose $f = S(h, g_0, \ldots, g_m)$ and Σ_1-terms $t, q_0, \ldots, q_m$ realize $h, g_0, \ldots, g_m$ respectively as follows: $h = t[x_0, \ldots, x_m]$, $g_0 =$

$= q_0 [z_1, \dots, z_k], \dots, g_m = q_m [z_1, \dots, z_k]$. Then the Σ_1-term $t_f = \mu w \exists x_0 \leqslant q_0 \dots \exists x_m \leqslant q_m (x_0 \approx q_0 \wedge \dots \wedge x_m \approx q_m \wedge w \approx t)$ obviously realizes f as follows: $f = t_f[z_1, \dots, z_k]$.

If $f = M(g)$ and $g = t_g [x_0, \dots, x_n]$ for Σ_1-term t_g, then it is easy to verify that for the Σ_1-term $t_f = \mu x_n (t_g \approx 0)$ $f = t_f[x_0, \dots, x_{n-1}]$.

Suppose $f = R(g, h)$ and $g = t_g [x_1, \dots, x_n]$, $h = t_h [x_1, \dots, x_{n+2}]$ for suitable Σ_1-terms t_g and t_h. Consider a Σ_1-formula φ defined as follows:

$$(\beta(u, 0) \approx t_g \wedge \forall w \leqslant x_{n+1} (\beta(u, s(w)) \approx (t_h)^{x_{n+1}, x_{n+2}}_{w, \beta(u, w)})),$$

where $u \neq w$ are variables distinct from the variables in $\{x_1, \dots, x_{n+2}\}$ and from all the variables occurring in t_g and t_h. Since $FV(t_g) \subseteq \{x_1, \dots, x_n\}$, $FV(t_h) \subseteq \{x_1, \dots, x_{n+2}\}$, we have $FV(\varphi) \subseteq \{u, x_1, \dots, x_{n+1}\}$. The preceding proposition shows that for any interpretation of variables $\eta: \{x_1, \dots, x_n\} \to \omega$ there is a value $n \in \omega$ of the variable u such that for $\eta' = \eta \cup \{\langle u, n \rangle\}$ $\varphi(\eta')$ is true. Consequently we can form a Σ_1-term $t_1 = \mu u \varphi$; $FV(t_1) \subseteq \subseteq \{x_1, \dots, x_{n+1}\}$. If we now set $t_f = \beta(t_1, x_{n+1})$, then $FV(t_f) \subseteq \subseteq \{x_1, \dots, x_{n+1}\}$ and it can easily be established by induction on the value of the variable x_{n+1} that $f = t_f[x_1, \dots, x_{n+1}]$. □

COROLLARY 1. *For any finite signature Σ and any recursive algebraic system Ω_Σ there is an effective procedure of changing every Σ-term or Σ-formula Θ into a recursive term or recursive formula Θ_0 so that $FV(\Theta) = FV(\Theta_0)$, and if $FV(\Theta) \subseteq \{x_1, \dots, x_n\}$, then $\Theta[x_1, \dots, x_n] = \Theta_0[x_1, \dots, x_n]$.*

This follows from Proposition 6 and Theorem 3. □

Exercises

1. Prove the recursiveness of a two-place function ex such that for $m, n \in \omega$, if $n \neq 0$, then $\mathrm{ex}(m, n) = m^n$ and $\mathrm{ex}(m, 0) = 1$.

2. Prove the recursiveness of a two-place function $|-|$ such that for any $n, m \in \omega$ $|n - m|$ is the absolute value of a difference of these numbers.

3. Prove that the one-place predicate $\{n \mid n \in \omega, n \text{ is a prime number}\}$ is recursive.

37. RECURSIVELY ENUMERABLE PREDICATES

In the preceding section we defined a recursive predicate to be a predicate whose representing function is recursive. Thus recursive predicates are precisely such predicates $R \subseteq \omega^n$ for which we can effectively solve the problem of occurrence, i. e. the problem of determining from a given n-tuple of numbers $\langle m_1, \ldots, m_n \rangle$ whether it is in the predicate R.

However, algorithmic procedures can be used for the process of generating a predicate (a set) $R \subseteq \omega^n$ itself as well as for recognizing the membership of the predicate. There are in general more such effectively generated predicates than recursive predicates. In this section we shall give a definition to the notion of recursively enumerable predicate which is an appropriate mathematical refinement of the concept of effectively generated predicate and study some basic properties of recursively enumerable predicates.

In the next section we shall see that there are indeed more recursively enumerable predicates than recursive ones.

We extend the class of recursive formulas to the class of *recursively enumerable formulas* using the following definition:

1. If φ is a recursive formula, then φ is a recursively enumerable formula.

2. If φ is a recursively enumerable formula and $x \in V$, then $\exists x\varphi$ is a recursively enumerable formula and $FV(\exists x\varphi) = FV(\varphi) \setminus \{x\}$.

In other words, recursively enumerable formulas are obtained from recursive formulas by quantification. For any recursively enumerable formula φ and interpretation $\eta\colon X \to \omega$, $FV(\varphi) \subseteq X \subseteq V$ there is a value $\varphi[\eta] \in \{T, F\}$ defined in a natural way; viz., if φ is representable as $\exists x_0 \exists x_1 \ldots \exists x_n \varphi_0$, where φ_0 is a recursive formula, $FV(\varphi_0) \subseteq FV(\varphi) \cup \{x_0, \ldots, x_n\}$, then $\varphi[\eta] = T$ if and only if there is an interpretation $\eta'\colon FV(\varphi_0) \to \omega$ such that $\eta'(v) = \eta(v)$ for all $v \in FV(\varphi)$ and $\varphi_0[\eta'] = T$.

Notice that according to Corollary 36.1 instead of recursive terms and formulas we may (and shall) use arbitrary Σ_1-terms and Σ_1-formulas as well.

With any recursively enumerable formula φ and a sequence of pairwise distinct variables $x_1, \dots, x_n$ such that $FV(\varphi) \subseteq \{x_1, \dots, x_n\}$ we can associate an n-place predicate $\varphi[x_1, \dots, x_n]$ as follows:

$$\varphi[x_1, \dots, x_n] = \{\langle m_1, \dots, m_n\rangle \mid \varphi[\eta] = T \quad \text{for } \eta = \{\langle x_i, m_i\rangle \mid i = 1, \dots, n\}\}.$$

The predicate $\varphi[x_1, \dots, x_n]$ is said to be *realized* by a recursively enumerable formula φ.

DEFINITION. A predicate $R \subseteq \omega^n$ is said to be *recursively enumerable* if it is realized by some recursively enumerable formula.

It can be seen from this definition and the results obtained earlier that any recursive predicate is recursively enumerable.

The notion of partially recursive predicate can be used to characterize partially recursive functions via the notion of graph. *The graph* of an n-place partial function f is an $(n + 1)$-place predicate Γ_f defined by the relation: for $m_1, \dots, m_n, k \in \omega$

$$\langle m_1, \dots, m_n, k\rangle \in \Gamma_f \Leftrightarrow f(m_1, \dots, m_n) = k.$$

THEOREM 4. (Graph). *A partial function f is partially recursive if and only if its graph Γ_f is recursively enumerable.*

We begin our proof with an auxiliary statement.

LEMMA. *For any n-place partially recursive predicate R there is a recursive formula φ such that $FV(\varphi) \subseteq \{x_0, x_1, \dots, x_n\}$ and $R = (\exists x_0 \varphi)[x_1, \dots, x_n]$.*

The lemma asserts that it may always be assumed that a recursively enumerable formula realizing a recursively enumerable predicate has only one existential quantifier. The proof of the lemma is obtained by induction on the number of existential quantifiers in a recursively enumerable formula using the following easily verifiable property:

For any recursive formula φ, $FV(\varphi) \subseteq \{x, y, x_1, \dots, x_n\}$,

$$(\exists x \exists y \varphi)[x_1, \dots, x_n] = (\exists x (\varphi)^{x,\, y}_{l(x),\, r(x)})[x_1, \dots, x_n].$$

Notice that $(\varphi)^{x,\, y}_{l(x),\, r(x)}$ is a Σ_1-formula. □

To prove necessity inductively we establish the following facts:

(1) The graphs of the basic functions are recursive:

$$\Gamma_o = (x \approx x \& y \approx 0)[x, y];$$
$$\Gamma_s = (s(x) \approx y)[x, y];$$
$$\Gamma_{I^n_m} = (x_m \approx y)[x_1, \ldots, x_n, y].$$

(2) Suppose $f = S(h, g_0, \ldots, g_n)$, the graphs $\Gamma_h, \Gamma_{g0}, \ldots, \Gamma_{g_n}$ of functions $h, g_0, \ldots, g_n$ respectively are recursively enumerable and $\varphi_h, \varphi_{g0}, \ldots, \varphi_{g_n}$ are recursive formulas such that

$$\Gamma_h = (\exists z \varphi_h)[u_0, \ldots, u_n, y];$$
$$\Gamma_{g0} = (\exists z_0 \varphi_{g0})[y_1, \ldots, y_k, u_0];$$
$$\vdots$$
$$\Gamma_{g_n} = (\exists z_n \varphi_{g_n})[y_1, \ldots, y_k, u_n],$$

with the variables $z, z_0, \ldots, z_n, y, y_1, \ldots, y_k, u_0, \ldots, u_n$ being pairwise distinct. Consider a recursive formula φ:

$$\varphi = \varphi_h \wedge \varphi_{g0} \wedge \ldots \wedge \varphi_{g_n}.$$

Then verification shows that

$$\Gamma_f = (\exists z \exists z_0 \ldots \exists z_n \exists u_0 \ldots \exists u_n \varphi)[y_1, \ldots, y_k, y].$$

Hence Γ_f is recursively enumerable.

(3) Suppose $f = R(h, g)$ and the graphs Γ_h, Γ_g of functions h, g respectively are recursively enumerable. Let φ_h and φ_g be recursive formulas such that

$$\Gamma_h = (\exists z_0 \varphi_h)[x_1, \ldots, x_n, y_0];$$
$$\Gamma_g = (\exists z_1 \varphi_g)[x_1, \ldots, x_{n+1}, x_{n+2}, y_1]$$

and let the variables $z_0, z_1, x_1, \ldots, x_n, x_{n+1}, x_{n+2}, y_0, y_1$ be pairwise distinct. Let us form the following Σ_1-formula φ:

$$\varphi = \forall x \leqslant x_{n+1}(((x \approx 0 \wedge (\varphi_h)^{y0\ \ z0}_{\beta(u,0)\ \beta(v,0)}) \vee$$
$$\vee (\neg x \approx 0 \wedge (\varphi_g)^{x_{n+1},\ x_{n+2},\ y_1,\ z_1}_{x \dot{-} 1,\ \beta(u,\, x \dot{-} 1),\ \beta(u,\, x),\ \beta(v,\, x)})) \wedge$$
$$\wedge\, y \approx \beta(u, x_{n+1}));$$

here u, v, y are pairwise distinct and differ from all the variables of the formulas φ_h, φ_g and from $z_0, z_1, x_1, \ldots, x_{n+2}$. Then $FV(\varphi) \subseteq \{u, v, y, x_1, \ldots, x_{n+1}\}$.

Let $\eta\colon \{u, v, y, x_1, \ldots, x_{n+1}\} \to \omega$ be such that $\varphi[\eta]$. We show that then $f(\eta x_1, \ldots, \eta x_{n+1})$ is defined and $f(\eta x_1, \ldots, \eta x_{n+1}) = \beta(\eta u, \eta x_{n+1}) = \eta y$. It will be shown by induction on $l \leqslant \eta x_{n+1}$ that $f(\eta x_1, \ldots, \eta x_n, l)$ is defined and $f(\eta x_1, \ldots, \eta x_n, l) = \beta(\eta u, l)$.

Let $l = 0$. Setting x equal to 0 we then see, since $\varphi(\eta) = T$, that a formula $(\varphi_h)^{y_0,\; z_0}_{\beta(u,\,0),\; \beta(v,\,0)}[\eta]$ must be true. And this means that $\langle \eta x_1, \ldots, \eta x_n, \beta(\eta u, 0)\rangle \in \Gamma_h$. Hence $h(\eta x_1, \ldots, \eta x_n)$ is defined and is equal to $\beta(\eta u, 0)$. But $f(\eta x_1, \ldots, \eta x_n, 0) = h(\eta x_1, \ldots, \eta x_n)$ as well. Hence $f(\eta x_1, \ldots, \eta x_n, 0)$ is defined and equals $\beta(\eta u, 0)$.

Suppose it has already been shown for $l < \eta x_{n+1}$ that $f(\eta x_1, \ldots, \eta x_n, l)$ is defined and equals $\beta(\eta u, l)$. Setting x equal to $l + 1$ $(\leqslant \eta x_{n+1})$ we see that a formula $(\varphi_g)^{x_{n+1},\; x_{n+2},\; y_1,\; z_1}_{x \dot{-} 1,\; \beta(u,\, x \dot{-} 1),\; \beta(u,\, x),\; \beta(v,\, x)}[\eta']$, where $\eta' = \eta \cup \{\langle x, l + 1\rangle\}$. In particular,

$$\langle \eta x_1, \ldots, \eta x_n, l, \beta(\eta u, l), \beta(\eta u, l + 1)\rangle \in \Gamma_g,$$

i. e. $g(\eta x_1, \ldots, \eta x_n, l, \beta(\eta u, l))$ is defined and equals $\beta(\eta u, l + 1)$; but since by the induction hypothesis $\beta(\eta u, l) = f(\eta x_1, \ldots, \eta x_n, l)$, it follows that $f(\eta x_1, \ldots, \eta x_n, l + 1) = g(\eta x_1, \ldots, \eta x_n, l, f(\eta x_1, \ldots, \eta x_n, l))$, is defined and equals $\beta(\eta u, l + 1)$.

Thus $f(\eta x_1, \ldots, \eta x_n, \eta x_{n+1})$ is defined and equals $\beta(\eta u, \eta x_{n+1})$. But since $(y \approx \beta(u, x_{n+1}))[\eta]$ is also true, we have $\eta y = \beta(\eta u, \eta x_{n+1})$.

Using the properties of the function β noted in Proposition 36.8 and the realizability of the graphs of the functions h and g by formulas $\exists z_0 \varphi_h$ and $\exists z_1 \varphi_g$ respectively it is easy to prove that if $m_1, \ldots, m_{n+1} \in \omega$ are such that $f(m_1, \ldots, m_{n+1})$ is defined and $f(m_1, \ldots, m_{n+1}) = k$, then there are $l, s \in \omega$ such that for an interpretation $\eta = \{\langle x_i, m_i\rangle \mid i = 1, \ldots, n + 1\} \cup \{\langle y, k\rangle, \langle u, l\rangle, \langle v, s\rangle\}$ $\varphi[\eta]$ is true.

Then from the above properties of a formula φ we see that the graph of f has a representation $\Gamma_f = (\exists u \exists v \varphi)\,[x_1, \ldots, x_{n+1}, y]$, i. e. the graph of f is recursively enumarable.

(4) Suppose $f = M(g)$ and the graph of Γ_g of a function g has a representation $\Gamma_g = (\exists z \varphi_g)[x_1, \ldots, x_{n+1}, y]$, where φ_g is a recursive formula.

Let φ be a Σ_1-formula defined as follows:

$$\varphi = \forall u \leqslant y((\varphi_g)^{x_{n+1},\ z,\ y}_{u,\ \beta(v,u),\ \beta(w,u)} \wedge$$
$$\wedge\, \beta(w, y) \approx 0 \wedge (u < y \rightarrow \neg \beta(w, u) \approx 0));$$

here u, v, w are distinct variables not occurring in φ_g. Proceeding as in the previous case it is not hard to verify that for the graph Γ_f of a function f the following relation is true:

$$\Gamma_f = (\exists v \exists w \varphi)[x_1, \ldots, x_n, y],$$

i. e. the graph of f is recursively enumerable.

To complete the proof of necessity we proceed by induction on the length of the determining sequence, using facts (1) to (4) established above.

Now we prove sufficiency. Suppose f is an n-place partial function and its graph Γ_f is recursively enumerable. Let φ be a recursive formula such that

$$\Gamma_f = (\exists z \varphi)[x_1, \ldots, x_n, y].$$

Consider a recursive predicate $\varphi[x_1, \ldots, x_n, y, z]$. By Proposition 36.5 this predicate is recursive, i. e. its representing function g is recursive. By the definition of a representing function:

for any $m_1, \ldots, m_n, k, l \in \omega$

$$\langle m_1, \ldots, m_n, k, l \rangle \in \varphi[x_1, \ldots, x_n, y, z] \Leftrightarrow$$
$$\Leftrightarrow g(m_1, \ldots, m_n, k, l) = 0.$$

A recursive $(n + 1)$-place function $h = g(I_1^{n+1}, \ldots, I_n^{n+1}, l(I_{n+1}^{n+1}), r(I_{n+1}^{n+1}))$ for any $m_1, \ldots, m_n, k$ satisfies the relation

$$h(m_1, \ldots, m_n, k) = g(m_1, \ldots, m_n, l(k), r(k)).$$

Let us consider a partially recursive function $f_0 = l(M(h))$ and show that it coincides with f.

Let $m_1, \ldots, m_n \in \omega$ be arbitrary. If $f(m_1, \ldots, m_n)$ is defined: $f(m_1, \ldots, m_n) = t \in \omega$, then $\langle m_1, \ldots, m_n, t \rangle \in \Gamma_f$. Consequently there is $s \in \omega$ such that $\langle m_1, \ldots, m_n, t, s \rangle \in \varphi[x_1, \ldots, x_n, y, z]$. Then $g(m_1, \ldots, m_n, t, s) = 0$ and for $k = c(t, s)$

$$h(m_1, \ldots, m_n, k) = g(m_1, \ldots, m_n, l(k), r(k)) =$$
$$= g(m_1, \ldots, m_n, t, s) = 0.$$

Hence $M(h)(m_1, \ldots, m_n)$ is defined. Let $M(h)(m_1, \ldots, m_n) = k_0$. Then $h(m_1, \ldots, m_n, k_0) = 0 = g(m_1, \ldots, m_n, l(k_0), r(k_0))$. Therefore $\langle m_1, \ldots, m_n, l(k_0), r(k_0)\rangle \in \varphi[x_1, \ldots, x_n, y, z]$, $\langle m_1, \ldots \ldots, m_n, l(k_0)\rangle \in (\exists z\varphi)[x_1, \ldots, x_n, y] = \Gamma_f$ and $f(m_1, \ldots, m_n) = = l(k_0) = f_0(m_1, \ldots, m_n)$ since $f_0(m_1, \ldots, m_n) = l(M(h)(m_1, \ldots \ldots, m_n)) = l(k_0)$. So if $f(m_1, \ldots, m_n)$ is defined, then $f_0(m_1, \ldots, m_n)$ is defined and $f(m_1, \ldots, m_n) = f_0(m_1, \ldots, m_n)$. Suppose $m_1, \ldots \ldots, m_n \in \omega$ and $f_0(m_1, \ldots, m_n)$ is defined. Then $M(h)(m_1, \ldots, m_n)$ is also defined and $f_0(m_1, \ldots, m_n) = l(M(h)(m_1, \ldots, m_n))$. Let $k \in \in \omega$ be such that $M(h)(m_1, \ldots, m_n) = k$. Then $h(m_1, \ldots, m_n, k) = = 0 = g(m_1, \ldots, m_n, l(k), r(k))$. Hence $\langle m_1, \ldots, m_n, l(k), r(k)\rangle \in \in \varphi[x_1, \ldots, x_n, y, z]$; $\langle m_1, \ldots, m_n, l(k)\rangle \in (\exists x\varphi)[x_1, \ldots, x_n, y] = = \Gamma_f$ and so $f(m_1, \ldots, m_n) = l(k)$.

Therefore if $f_0(m_1, \ldots, m_n)$ is defined, then so is $f(m_1, \ldots \ldots, m_n)$ and $f_0(m_1, \ldots, m_n) = l(M(h)(m_1, \ldots, m_n)) = l(k) = = f(m_1, \ldots, m_n)$. Thus $f = f_0$ and hence f is a partially recursive function. ☐

COROLLARY 1. *For any n-place partially recursive function f there is an* $(n + 1)$*-place recursive function h such that given any* $m_1, \ldots, m_n$

$$f(m_1, \ldots, m_n) = l(M(h)(m_1, \ldots, m_n)).$$

It is immediate from the proof of sufficiency in the theorem. ☐

COROLLARY 2. *A partially recursive function is recursive if and only if it is completely defined.*

Necessity is obvious. Sufficiency follows immediately from the preceding corollary. ☐

We shall call one-place predicates simply sets. Accordingly recursive (recursively enumerable) one-place predicates are *recursive* (*recursively enumerable*) *sets*.

We prove the basic structural properties of recursive and recursively enumerable sets.

PROPOSITION 1. (a) *If a set X is recursive, then X is recursively enumerable.*

(b) *A finite set is recursive.*

(c) *If X, Y are recursive* (*recursively enumerable*) *sets, then* $X \cup Y$ *and* $X \cap Y$ *are also recursive* (*recursively enumerable*) *sets.*

(d) *For a recursively enumerable set X $\omega \setminus X$ is a recursively enumerable set if and only if X is a recursive set.*

PROOF. Statement (a) was noted earlier for predicates with an arbitrary number of places.

(b) If $X = \varnothing$, then the representing function for X is $\mathrm{sg}(s)$. If $X = \{n\}$, then the function $\delta(\underline{n}, x)[x]$ is the representing function for X. If $X = \{n_0, n_1, \ldots, n_k\}$, $k > 0$, then the representing function for X is a function

$$(\delta(n_0, x) \cdot \delta(n_1, x) \cdot \ \ldots \ \cdot \delta(n_k, x))[x].$$

(c) If X and Y are recursive and g, h are the representing functions for X and Y respectively, then $g \cdot h$ is the representing function for $X \cup Y$ and $\mathrm{sg}(g + h)$ is the representing function for $X \cap Y$.

Suppose X and Y are recursively enumerable sets and φ_0, φ_1 are recursive formulas such that $X = (\exists z_0 \varphi_0)[x]$, $Y = (\exists z_1 \varphi_1)[x]$ and x, z_0, z_1 are pairwise distinct variables. Then

$$X \cup Y = (\exists z_0 \exists z_1 (\varphi_0 \vee \varphi_1))[x];$$
$$X \cap Y = (\exists z_0 \exists z_1 (\varphi_0 \wedge \varphi_1))[x],$$

i. e. $X \cup Y$ and $X \cap Y$ are realized by recursively enumerable formulas and so are recursively enumerable.

(d) If X is a recursive set and g is the recursive representing function for X, then $\overline{\mathrm{sg}}(g)$ is the recursive representing function for $\omega \setminus X$.

Suppose now that X and $\omega \setminus X$ are recursively enumerable sets. Let φ_0, φ_1 be recursive formulas such that

$$X = (\exists z \varphi_0)[x] \qquad \text{and} \qquad \omega \setminus X = (\exists z \varphi_1)[x].$$

It may be assumed without loss of generality that φ_0 and φ_1 contain no bound occurrences of x. Consider a recursive formula $\varphi = (\varphi_0 \vee \varphi_1)$; $FV(\varphi) \subseteq \{x, z\}$. For any value n of a variable x there is a value m of a variable z such that given $\eta = \{\langle x, n\rangle, \langle z, m\rangle\}$ we have $\varphi[\eta] = T$. Indeed, if $n \in X$, then there is a value m for z such that $\varphi_0[\eta] = T$. But if $n \in \omega \setminus X$, then we can find a value m for z such that $\varphi_1[\eta] = T$. Hence $\mu z \varphi$ is a recursive term and $(\varphi_0)^z_{\mu z \varphi}$ is a recursive formula. We verify that $X = (\varphi_0)^z_{\mu z \varphi}[x]$. Let $h = \mu z \varphi[x]$ be a recursive function. Then by construction for any $n \in \omega$, for $\eta = \{\langle x, n\rangle, \langle z, h(n)\rangle\}\ \varphi[\eta] = T$. Also note that for $\eta_0 = \{\langle x, n\rangle\}\ (\varphi_0)^z_{\mu z\varphi}[\eta_0] = \varphi_0[\eta]$. If $n \in X$, then $\varphi_1[\eta]$ cannot be true, since otherwise $n \in \omega \setminus X$. Hence $\varphi_0[\eta]$ and $(\varphi_0)^z_{\mu z\varphi}[\eta_0]$ are true and $n \in (\varphi_0)^z_{\mu z\varphi}[x]$. If $n \in \omega \setminus X$, then $\varphi_0[\eta]$ cannot be true. Hence $(\varphi_0)^z_{\mu z\varphi}[\eta_0] = F$ and $n \notin (\varphi_0)^z_{\mu z\varphi}[x]$. So the set X is realized by the recursive formula $(\varphi_0)^z_{\mu z\varphi}$. Hence X is recursive. □

We now give a characterization of recursively enumerable sets using recursive functions.

PROPOSITION 2. *A nonempty set X is recursively enumerable if and only if there is a one-place recursive function f such that $X = \{f(n) \mid n \in \omega\}$.*

PROOF. Suppose X is recursively enumerable and $n_0 \in X$. Let φ be a recursive formula such that $X = (\exists y\varphi)[x]$. Then $FV(\varphi) \subseteq \{x, y\}$. Consider a Σ_1-formula ψ:

$$\psi = (\varphi^{x,\ y}_{l(x),\ r(x)} \wedge z \approx l(x)) \vee (\neg\varphi^{x,\ y}_{l(x),\ r(x)} \wedge z \approx n_0);$$

$FV(\psi) \subseteq \{x, z\}$ and for any value k of x there is a value s of z such that given $\eta = \{\langle x, k\rangle, \langle z, s\rangle\}\ \psi[\eta] = T$. Indeed, if given $\eta_0 = \{\langle x, k\rangle\}\ \varphi^{x,\ y}_{l(x),\ r(x)}[\eta_0]$, then as s we may take $l(k)$. But if we have $\neg\varphi^{x,\ y}_{l(x),\ r(x)}[\eta_0]$, then as s we may take n_0. Hence $\mu z\varphi$ is a Σ_1-term and the recursive function $f = \mu z\psi[x]$ it realizes satisfies the conclusion of the proposition. Indeed, if $k \in X$, then there is $s \in \omega$ such that for $\eta = \{\langle x, k\rangle, \langle y, s\rangle\}\ \varphi[\eta]$. Hence given $t = c(k, s)$, $\eta_0 = \{\langle x, t\rangle\}\ \varphi^{x,\ y}_{l(x),\ r(x)}[\eta_0] = \varphi[\eta] = T$ and so $f(t) = l(t) = l(c(k, s)) = k$. Thus $X \subseteq \{f(t) \mid t \in \omega\}$. Conversely, if $f(t) = k$, then for $\eta = \{\langle x, t\rangle, \langle z, k\rangle\}\ \psi[\eta]$ and therefore either $\langle l(t), r(t)\rangle \in \varphi[x, y]$ and so $k = l(t) \in X$ or $\langle l(t), r(t)\rangle \notin \varphi[x, y]$ and so $k = n_0 \in X$. Thus $\{f(t) \mid t \in \omega\} \subseteq X$ and $X = \{f(t) \mid t \in \omega\}$.

Sufficiency will follow from a more general statement.

The range of any one-place partially recursive function f, i. e. the set $R_f = \{k \mid$ there is $n \in \omega$, $f(n)$ is defined and $f(n) = k\}$, is recursively enumerable.

Indeed, let φ be a recursively enumerable formula realizing the graph Γ_f of a function f: $\Gamma_f = \varphi[x, y]$. Then obviously $R_f = (\exists x\varphi)[y]$. □

Suppose given an n-place partial function f Δ_f denotes the domain of f, i.e. an n-place predicate $\{\langle m_1, \ldots, m_n\rangle\ m_1, \ldots, m_n \in \omega,$ $f(m_1, \ldots, m_n)$ is defined$\}$.

PROPOSITION 3. *For any n-place partially recursive function f its domain Δ_f is a recursively enumerable predicate.*

PROOF. Let φ be a recursively enumerable formula realizing the graph Γ_f of a function f: $\Gamma_f = \varphi[x_1, \ldots, x_n, y]$. Then obviously $\Delta_f = (\exists y\varphi)[x_1, \ldots, x_n]$. □

PROPOSITION 4. (Reduction Theorem). *For any two recursively enumerable sets* R_0 and R_1 *there are recursively enumerable sets* R_0 and R_1 *such that* $R_0' \subseteq R_0$, $R_1' \subseteq R_1$, $R_0' \cap R_1' = \varnothing$ and $R_0 \cup R_1 = R_0' \cup R_1'$.

PROOF. Let φ_0, φ_1 be recursive formulas such that $R_0 = (\exists z\varphi_0)[x]$ and $R_1 = (\exists z\varphi_1)[x]$. Consider recursive formulas:

$$\varphi_0' = \varphi_0 \wedge \forall y \leqslant z(y \approx z \vee \neg(\varphi_1)_y^z);$$
$$\varphi_1' = \varphi_1 \wedge \forall y \leqslant z\ \neg(\varphi_0)_y^z.$$

Then $R_0' = (\exists z\varphi_0')[x]$ and $R_1' = (\exists x\varphi_1')[x]$ will be the required sets. Indeed, the inclusions $R_0' \subseteq R_0$ and $R_1' \subseteq R_1$ are obvious, since $\varphi_i{}'$ implies φ_i, $i = 0, 1$. Let $n \in R_0 \cup R_1$. Then there is a least s such that $(\varphi_0 \vee \varphi_1)$ is true for $\eta = \{\langle x, n\rangle, \langle z, s\rangle\}$. If $\varphi_0[\eta]$ holds, then so obviously does $\varphi_0'[\eta]$ and therefore $n \in R_0'$. If, however, $\neg\varphi_0[\eta]$ is true, then so is $\varphi_1'[\eta]$ and therefore $n \in R_1'$. So $R_0 \cup R_1 = R_0' \cup R_1'$. Suppose now that $k \in R_0' \cap R_1'$ and $s_0, s_1 \in \omega$ are such that for $\eta_0 = \{\langle x, k\rangle, \langle z, s_0\rangle\}$, $\eta_1 = \{\langle x, k\rangle, \langle z, s_1\rangle\}$ we have $\varphi_0'[\eta_0]$ and $\varphi_1'[\eta_1]$. Suppose first that $s_1 < s_0$. Then since $\forall y \leqslant z(y \approx z \vee \neg(\varphi_1)_y^z)[\eta_0]$ is true, so must be $\neg\varphi_1[\eta_1]$ and of course $\neg\varphi_1'[\eta_1]$. But if $s_0 \leqslant s_1$, then the truth of $\forall y \leqslant z\ \neg\ (\varphi_0)_y^z[\eta_1]$ implies that we have $\neg\varphi_0[\eta_0]$ and of course $\neg\varphi_0'[\eta_0]$. A contradiction which shows that $R_0' \cap R_1' = \varnothing$. □

PROPOSITION 5 (Uniformization Theorem). *Let R be an arbitrary* $(n + 1)$*-place recursively enumerable predicate. Then there is an n-place partially recursive function f such that* $\Gamma_f \subseteq R$ and $\Delta_f = R' = \{\langle m_1, \ldots, m_n\rangle \mid$ *there is* $m_{n-1} \in \omega$ *such that* $\langle m_1, \ldots, m_n, m_{n+1}\rangle \in R\}$.

PROOF. Let φ be a recursive formula such that $R = (\exists y\varphi)[x_1, \ldots, x_n, x_{n+1}]$. Let $u \neq z$ be variables not occurring in φ. Consider a recursive formula ψ defined as follows:

$$\psi = y \approx l(z) \wedge (\varphi)^{x_{n+1},\, y}_{l(z),\, r(z)} \wedge \forall u \leqslant z(u \approx z \vee \neg (\varphi)^{x_{n+1},\, y}_{l(u),\, r(u)}).$$

Then $R_0 = (\exists z\psi)[x_1, \ldots, x_n, y]$ is the graph Γ_f of some (partially recursive) function f, $\Gamma_f \subseteq R$ and $\Delta_f = R' = \{\langle m_1, \ldots, m_n \rangle \mid$ there is $m_{n+1} \in \omega$ such that $\langle m_1, \ldots, m_{n+1} \rangle \in R\}$. This follows easily from the following facts:

(1) *if* $\langle m_1, \ldots, m_n \rangle \in R'$ *and* k *is a least natural number such that for* $\eta = \{\langle x_1, m_1 \rangle, \ldots, \langle x_n, m_n \rangle, \langle x_{n+1}, l(k)\rangle, \langle y, r(k)\rangle\}$ *we have* $\varphi[\eta]$, *then* $\psi[\eta_0]$ *holds for* $\eta_0 = \{\langle x_1, m_1 \rangle, \ldots$ $\ldots, \langle x_n, m_n \rangle, \langle z, k \rangle, \langle y, l(k)\rangle\}$;

(2) *if* $\eta_0 : \{x_1, \ldots, x_n, z, y\} \to \omega$, $\eta_1 : \{x_1, \ldots, x_n, z, y\} \to \omega$ *are such that* $\eta_0(x_i) = \eta_1(x_i)$, $1 \leqslant i \leqslant n$, *and* $\psi[\eta_0]$, $\psi[\eta_1]$ *are true, then* $\eta_0 = \eta_1$;

(3) *if for* $\eta_0 : \{x_1, \ldots, x_n, z, y\} \to \omega$ *we have* $\psi[\eta_0]$, *then for* $\eta = \{\langle x_1, \eta_0 x_1 \rangle, \ldots, \langle x_n, \eta_0 x_n \rangle \langle x_{n+1}, \eta_0 y\rangle, \langle y, r(\eta_0 z)\rangle\}$ *we have* $\varphi[\eta]$.

The facts are directly verified proceeding from the definition of ψ. □

With every $(n + 1)$-place predicate R, $n > 0$, we can associate a family of n-place predicates obtained from R by cuts in the following way:

given any $k \in \omega$ let $R_k = \{\langle m_1, \ldots, m_n \rangle \mid \langle k, m_1, \ldots, m_n \rangle \in$ $\in R\}$; the predicate R_k is a *k-cut of R*.

It can easily be seen that if R is a recursive or a recursively enumerable predicate, then for any $k \in \omega$ R_k is also a recursive or a recursively enumerable predicate respectively.

An $(n + 1)$-place recursively enumerable predicate R is said to be *universal for n-place recursively enumerable predicates* if a family $\{R_k \mid k \in \omega\}$ of cuts of R coincides with the family of all n-place recursively enumerable predicates. In the next section we shall prove the existence of universal $(n + 1)$-place recursively enumerable predicates for any $n > 0$.

Similarly, with every $(n + 1)$-place partially recursive function f, $n > 0$, we can associate a family of n-place partial functions f_k, $k \in \omega$, assuming for $m_1, \ldots, m_n \in \omega$

$$f_k(m_1, \ldots, m_n) = f(k, m_1, \ldots, m_n).$$

It is clear that if f is a partially recursive function, then so is f_k for any $k \in \omega$.

An $(n + 1)$-place partially recursive function f is said to be *universal for n-place partially recursive functions* if $\{f_k \mid k \in \omega\}$ coincides with the family of all n-place partially recursive functions.

Now note that the existence of universal partially recursive functions is a consequence of the existence of universal recursively enumerable predicates.

PROPOSITION 6. *If R is an $(n + 2)$-place recursively enumerable predicate universal for $(n + 1)$-place recursively enumerable predicates, $n > 0$ and f is an $(n + 1)$-place partially recursive function uniformizing R, i. e. such that $\Gamma_f \subseteq R$ and $\Delta_f = R' =$ $= \{\langle m_1, \ldots, m_{n+1}\rangle \mid$ there is $m_{n+2} \in \omega$ such that $\langle m_1, \ldots$ $\ldots, m_{n+1}, m_{n+2}\rangle \in R\}$, then f is universal for n-place partially recursive functions.*

PROOF. Let g be an n-place partially recursive function. Then the graph Γ_g of g is an $(n + 1)$-place recursively enumerable predicate. Hence there is $k \in \omega$ such that $\Gamma_g = R_k = \{\langle m_1, \ldots$ $\ldots, m_{n+1}\rangle \mid \langle k, m_1, \ldots, m_{n+1}\rangle \in R\}$. Consider a function f_k. We show that $g = f_k$.

Suppose $f_k(m_1, \ldots, m_n)$ is defined and equals $l \in \omega$. Then $f(k, m_1, \ldots, m_n) = l$ and $\langle k, m_1, \ldots, m_n, l\rangle \in R$ and hence $\langle m_1, \ldots, m_n, l\rangle \in R_k = \Gamma_g$. Therefore $g(m_1, \ldots, m_n)$ is defined and equals l. Conversely, suppose $g(m_1, \ldots, m_n)$ is defined and equals l. Then $\langle m_1, \ldots, m_n, l\rangle \in \Gamma_g = R_k$, $\langle k, m_1, \ldots, m_n, l\rangle \in R$, $\langle k, m_1, \ldots, m_n\rangle \in R'$ and hence $f(k, m_1, \ldots, m_n)$ is defined and, as shown above, $f_k(m_1, \ldots, m_n) = f(k, m_1, \ldots, m_n) = l =$ $= g(m_1, \ldots, m_n)$.

Thus $g = f_k$. Since g is arbitrary, it follows that $\{f_k \mid k \in \omega\}$ consists of all n-place partially recursive functions. ☐

We conclude this section by considering a notion that can be used for a comparison of recursively enumerable sets with predicates in terms of their "algorithmic" complexity. This concept relates to the family of notions of reducibility in the theory of algorithms and is one of the best justified intuitively.

Suppose R is an n-place predicate, $n > 0$, and X is a set. We say that *R is m-reducible to X* if there is an n-place recursive function f such that for any $m_1, \ldots, m_n \in \omega$

$$\langle m_1, \ldots, m_n \rangle \in R \Leftrightarrow f(m_1, \ldots, m_n) \in X.$$

Every recursive function f satisfying this condition is *a reducing function for R and X*.

If R is m-reducible to X, then this is designated $R \leqslant_m X$.

We formulate the simplest properties of this notion in the form of a statement.

PROPOSITION 7. *If R is an n-place predicate, X, X_0, X_1 are sets, $R \leqslant_m X$. Then*

(1) *if X is a recursive or recursively enumerable set, then R is a recursive or recursively enumerable predicate respectively*;

(2) $X \leqslant_m X$; *if* $X \leqslant_m X_0$, $X_0 \leqslant_m X_1$, *then* $X \leqslant_m X_1$;

(3) *any recursive predicate Q m-reduces to any set X distinct from $\varnothing$ and ω.*

PROOF. (1) Let f be a reducing function (for R and X). If X is recursive and χ_X is the characteristic function of X, then $\chi_X(f)$ is the characteristic (recursive!) function of R. If X is recursively enumerable, then suppose that φ is a recursive formula realizing X as follows: $X = (\exists z\varphi)[x]$. Let t be a recursive term realizing a function f as follows: $f = t[x_1, \ldots, x_n]$. Then it is easily seen that

$$R = (\exists x \exists z(t \approx x \wedge \varphi))[x_1, \ldots, x_n].$$

Hence R is realized by a recursively enumerable formula.

Statement (2) of Proposition 7 is obvious.

(3) Suppose $n_0 \notin X$, $n_1 \in X$ and f is any one-place recursive function assuming a value n_0 at zero and a value n_1 at unity. If χ_R is the (recursive) characteristic function of R, then $f(\chi_R)$ is a reducing function for R and X. □

In the next section we shall show that there are sets among recursively enumerable sets that are greatest with respect to m-reducibility; more precisely, recursively enumerable sets X_0 such that for any recursively enumerable set X $X \leqslant_m X_0$; such sets will be called *m-universal recursively enumerable sets*.

Power-set considerations show that there can be no set among all sets that is greatest with respect to m-reducibility, since no more than a countable family of sets (a set of recursive functions is countable!) can m-reduce to a fixed set.

Exercises

For a two-place predicate $R \subsetneq \omega^2$ we denote by $c(R)$ a set $\{n \mid n \in \omega,\ \langle l(n), r(n)\rangle \in R\}$.

1. Prove that a mapping $R \mapsto c(R)$ is a one-to-one correspondence between all two-place predicates and subsets of ω.

2. Prove that $R \subsetneq \omega^2$ is a recursive predicate if and only if $c(R)$ is a recursive set.

3. Prove that $R \subsetneq \omega^2$ is a recursively enumerable predicate if and only if $c(R)$ is a recursively enumerable set.

4. Suppose that $n_0, \ldots, n_m \in \omega$ are pairwise distinct and that $k_0, \ldots, k_m \in \omega$ are arbitrary. Prove that there is a one-place recursive function f such that $f(n_i) \leqslant k_i$ for all $i = m$. (*Hint*. Make use of the graph theorem.)

5. Prove that there is no $(n + 1)$-place recursive predicate R_n universal for the family of all n-place recursive predicates. (*Hint*. For an $(n + 1)$-place recursive predicate R_n consider an n-place recursive predicate $\{\langle m_1, \ldots, m_n\rangle \langle m_1, m_1, \ldots \ldots, m_n\rangle \notin R_n\}$.)

38. UNDECIDABILITY OF THE CALCULUS OF PREDICATES AND GÖDEL'S INCOMPLETENESS THEOREM

The question of decidability is one of the most important questions when studying a calculus.

A calculus I is said *to be decidable* if there is an algorithm that allows one to find out from any expression Φ whether or not Φ is a theorem of I. Otherwise the calculus I is said *to be undecidable.*

A Gödel numbering of a set X of words of an alphabet A is a distinct-valued mapping $g\colon X \to \omega$ such that there is an algorithm G computing from a word $\alpha \in X$ its number $g(\alpha)$ and there is an algorithm G_1 writing out from a number $n \in \omega$ a word α if $n = g(\alpha)$ and producing a number 0 if $n \in \omega \setminus \{g(\alpha) \mid \alpha \in X\}$.

It is clear that by Church's thesis the question of decidability of a calculus I with a Gödel numbering g of all the expressions of I reduces to that of the recursiveness of the set $\{g(\Phi) \mid \Phi \text{ is a theorem of } I\}$.

Consider a signature $\Sigma_0 = \langle <^2;\ +^2,\ \cdot^2,\ s^1,\ 0\rangle$ consisting of the symbol $<$ of a two-place relation, of the symbols $+$, $\cdot$ of two-place functions, of the symbol s of a one-place function and of the symbol 0 of a constant. By induction on the construction of terms and formulas we define a Gödel numbering $\gamma\colon T(\Sigma_0) \cup F(\Sigma_0) \to \omega$ of the terms and formulas of Σ_0:

(1) $\gamma(0) = c(0, 1)$,
(2) $\gamma(v_i) = c(1, i)$,
(3) $\gamma(s(t)) = c(2, \gamma t)$,
(4) $\gamma(t + q) = c(3, c(\gamma t, \gamma q))$,
(5) $\gamma(t \cdot q) = c(4, c(\gamma t, \gamma q))$,
(6) $\gamma(t \approx q) = c(5, c(\gamma t, \gamma q))$,
(7) $\gamma(t < q) = c(6, c(\gamma t, \gamma q))$,
(8) $\gamma(\Phi \wedge \Psi) = c(7, c(\gamma\Phi, \gamma\Psi))$,
(9) $\gamma(\Phi \vee \Psi) = c(8, c(\gamma\Phi, \gamma\Psi))$,
(10) $\gamma(\Phi \to \Psi) = c(9, c(\gamma\Phi, \gamma\Psi))$,
(11) $\gamma(\neg\Phi) = c(10, \gamma\Phi)$,
(12) $\gamma(\exists v_i \Phi) = c(11, c(i, \gamma\Phi))$,
(13) $\gamma(\forall v_i \Phi) = c(12, c(i, \gamma\Phi))$.

Since the functions c, r, l are computable, it is easy to see that γ is a Gödel numbering of the terms and formulas of Σ_0.

In what follows a set $X \subseteq T(\Sigma_0) \cup F(\Sigma_0)$ is said *to be recursive* (*recursively enumerable*) if $\gamma[X]$ is a recursive (recursively enumerable) set.

We shall have to establish the recursiveness of a great number of functions below. Before proceeding therefore we first present a purely technical result to be constantly used in what follows.

For any $(n + 1)$-place function f an $(n + 1)$-place function $\bar{f}$ is defined as follows: for any $m_1, \dots, m_n, m_{n+1} \in \omega$ $\bar{f}(m_1, \dots, m_n, m_{n+1})$ is a least number $k \in \omega$ such that we have: $\beta(k, 0) = f(m_1, \dots, m_n, 0)$, $\beta(k, 1) = f(m_1, \dots, m_n, 1), \dots, \beta(k, m_{n+1}) = f(m_1, \dots, m_n, m_{n+1})$.

If f is recursive, then so is $\bar{f}$, for if $f = t[x_1, \dots, x_n, x_{n+1}]$, where t is a recursive term, then $\bar{f} = q[x_1, \dots, x_n, x_{n+1}]$, where

$$q = \mu y(\forall z \leqslant x_{n+1}(\beta(y, z) \approx (t)_z^{x_{n+1}}))$$

is a recursive term. Conversely, if $\bar{f}$ is recursive, then f is recursive since $f(m_1, \dots, m_n, m_{n+1}) = \beta(\bar{f}(m_1, \dots, m_n, m_{n+1}), m_{n+1})$.

PROPOSITION 1. *Suppose we are given numbers* $k, n_0, \dots, n_k \in \omega$, *recursive functions* $f^{n+1}, f_0^{n+n_0+1}, \dots, f_k^{n+n_k+1}$, *with the number of places shown by a superscript, one-place recursive functions* $g_{0,1}, \dots, g_{0,n_0}, \dots, g_{k,1}, \dots, g_{k,n_k}$ *and recursive for-*

mulas $\varphi_0, \ldots, \varphi_k$; $FV(\varphi_i) \subseteq \{x_1, \ldots, x_n, y\}$, $i \leqslant k$. *Let the following conditions hold for any interpretation* η: $\{x_1, \ldots, x_n, y\} \to \omega$ *and any* $i \leqslant k$:

(a) *if* $\varphi_i[\eta]$, *then* $\neg \varphi_j[\eta]$ *for any* $j \leqslant k, j \neq i$;

(b) *if* $\varphi_i[\eta]$ *and* $n_i \neq 0$, then $g_{i,j}(\eta(y)) < \eta(y)$ *for all* $j \in \{1, \ldots, n_i\}$.

Then there is a unique recursive function h satisfying the condition: for any $m_1, \ldots, m_n, l \in \omega$, *if* $\eta = \{\langle x_i, m_i\rangle \mid 1 \leqslant i \leqslant n\} \cup \{\langle y, l\rangle\}$, *then* $h(m_1, \ldots, m_n, l) =$

$$= \begin{cases} f_0(m_1, \ldots, m_n, l, h(m_1, \ldots, m_n, g_{0,1}(l)), \ldots \\ \qquad \ldots, h(m_1, \ldots, m_n, g_{0,n_0}(l))), \text{ if } \varphi_0[\eta]; \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ f_k(m_1, \ldots, m_n, l, h(m_1, \ldots, m_n, g_{k,1}(l)), \ldots \\ \qquad \ldots, h(m_1, \ldots, m_n, g_{k,n_k}(l))), \text{ if } \varphi_k[\eta]; \\ f(m_1, \ldots, m_n, l) \text{ otherwise.} \end{cases}$$

PROOF. The existence and uniqueness of a function h satisfying the condition of the proposition are easily established by induction on the last independent variable using the conditions on φ_i, $i \leqslant k$, and $g_{i,j}$. It will be proved below that the function $\bar{h}$ is realized by some Σ_1-term. Once this fact has been established, the recursiveness of h will follow from the relation between h and $\bar{h}$ noted above and from Proposition 36.5.

Let the following relations hold for suitably chosen recursive terms $q, t_0, \ldots, t_k, r_{0,1}, \ldots, r_{k,n_k}$:

$$f = q[x_1, \ldots, x_n, y];$$
$$f_0 = t_0[x_1, \ldots, x_n, y, z_1, \ldots, z_{n_0}];$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$f_k = t_k[x_1, \ldots, x_n, y, z_1, \ldots, z_{n_k}];$$
$$g_{i,j} = r_{i,j}[y], \quad i \leqslant k, j \in \{1, \ldots, n_i\}.$$

Suppose $s_{ij} = \beta(z, r_{i,j})$, $i \leqslant k, j \in \{1, \ldots, n_i\}$; $s_{i,j}$ are Σ_1-terms and $FV(s_{i,j}) \subseteq \{z, y\}$.

Consider the following Σ_1-formula φ:

$$\Big(\bigwedge_{i \leqslant k} (\varphi_i \to \beta(z, y) \approx (t_i)^{z_1, \ldots, z_{n_i}}_{s_{i,1}, \ldots, s_{i,n_i}}) \Big) \wedge$$
$$\wedge \Big(\bigwedge_{i \leqslant k} \neg \varphi_i \to \beta(z, y) \approx q \Big).$$

Then $FV(\varphi) \subseteq \{x_1, \ldots, x_n, y, z\}$. Set $\psi = \forall w \leqslant y(\varphi)^y_w$, $FV(\psi) = FV(\varphi)$. We show that

for an interpretation $\eta = \{\langle x_i, m_i\rangle \mid i = 1, \ldots, n\} \cup \{\langle y, l\rangle\}$ *and for a number* $j \in \omega$ *the following conditions are equivalent*:

(1) $\psi[\eta']$ *is true, where* $\eta' = \eta \cup \{\langle z, j\rangle\}$;

(2) *for any* $m \leqslant l$ $\beta(j, m) = h(m_1, \ldots, m_n, m)$.

Suppose that for $l' < l$ the equivalence of conditions (1) and (2) has been proved (with l replaced by l'). We prove this equivalence for l.

Let condition (1) hold. Then it is easily seen from the form of the formula ψ that if $l' < l$, $\eta'' = (\eta' \setminus \{\langle y, l\rangle\}) \cup \{\langle y, l'\rangle\}$, then $\psi[\eta'']$. By the induction hypothesis therefore it may be assumed that $\beta(j, m) = h(m_1, \ldots, m_n, m)$ for all $m < l$.

Consider the case where there is $i \leqslant k$ such that $\varphi_i[\eta]$ is true. Then from the truth of $\psi[\eta']$ and $\varphi[\eta']$ it follows that

$$\beta(j, l) = \beta(z, y)[\eta'] = (t_i)^{z_1, \ldots, z_{n_i}}_{s_{i,1}, \ldots, s_{i,n_i}}[\eta'] =$$
$$= f_i(m_1, \ldots, m_n, l, s_{i,1}, [\eta'], \ldots, s_{i,n_i}[\eta']). \qquad (*)$$

Further, for $j' \in \{1, \ldots, n_i\}$ $s_{i,j'}[\eta'] = \beta(j, r_{i,j'}[\eta']) = \beta(j, g_{i,j'}(l))$. Since $\varphi_i[\eta]$ is true, by condition (b) of Proposition 1 $g_{i,j'}(l) < l$ (if $n_i \neq 0$). Hence $\beta(j, g_{i,j'}(l)) = h(m_1, \ldots, m_n, g_{i,j'}(l))$ and therefore

$$\beta(j, l) = f_i(m_1, \ldots, m_n, l, h(m_1, \ldots, m_n, g_{i,1}(l), \ldots$$
$$\ldots, h(m_1, \ldots, m_n, g_{i,n_i}(l) = h(m_1, \ldots, m_n, l).$$

If for any $i \leqslant k$ $\neg\varphi_i[\eta]$, then from the truth of $\psi[\eta']$ we get

$$\beta(j, l) = \beta(z, y)[\eta'] = q[\eta'] = f(m_1, \ldots, m_n, l) =$$
$$= h(m_1, \ldots, m_n, l). \qquad (**)$$

So whenever $\psi[\eta']$ is true, for any $m \leqslant l$ $\beta(j, m) = h(m_1, \ldots, m_n, m)$.

Conversely, let $j \in \omega$ be such that for all $m \leqslant l$ $\beta(j, m) = h(m_1, \ldots, m_n, m)$. Then, using these equations and relations $(*)$ and $(**)$, we see that $\varphi[\eta']$ is true. If, however, $l' < l$ and $\eta'' = (\eta' \setminus \{\langle y, l\rangle\}) \cup \{\langle y, l'\rangle\}$, then $\varphi[\eta'']$ is true by the induction hypothesis about the equivalence of conditions (1) and (2).

For $\eta = \{\langle x_i, m_i\rangle | i = 1, \ldots, n\} \cup \{\langle y, l\rangle\}$ therefore $(\mu z\psi)[\eta]$ is a least $j \in \omega$ such that for all $m \leqslant l\ \beta(j, m) = h(m_1, \ldots, m_n, m)$. By the definition of $\overline{h}$ we get $\overline{h}(m_1, \ldots, m_n, l) = (\mu z\psi)[\eta]$. Hence $\overline{h} = (\mu z\psi)[x_1, \ldots, x_n, y]$. As was noted at the beginning of the proof, this already implies the recursiveness of h. □

The function h of Proposition 1 is said to be defined by *reflexive recursion according to a piecewise scheme* or to be defined by *piecewise reflexive recursion*. In a definition according to a piecewise reflexive recursion, instead of formulas φ_i we shall often write conditions that can be easily expressed by a formula (for example, $3 \leqslant x \leqslant 9$, $x \neq 2$ and so on).

PROPOSITION 2. *The following sets are recursive*:

(a) *the set* $T(\Sigma_0)$ *of terms of* Σ_0;

(b) *the set* $F(\Sigma_0)$ *of formulas of* Σ_0;

(c) *the set* $A(\Sigma_0)$ *of axioms of* $CP_1^{\Sigma_0}$.

PROOF. We write out the definition of a piecewise reflexive recursion for the characteristic function T of a set $\gamma(T(\Sigma_0))$:

$$T(n) = \begin{cases} 1, \text{ if } n = c(0, 1) \text{ or } l(n) = 1 \\ T(r(n)) \text{ if } l(n) = 2 \\ T(lr(n)) \cdot T(rr(n)) \text{ if } 3 \leqslant l(n) \leqslant 4 \\ 0 \text{ otherwise.} \end{cases}$$

Notice that from the definitions of c, l, r we get $l(n) \leqslant n$, $r(n) \leqslant n$ and $k, m < c(k, m)$ for $k \geqslant 2$.

For the characteristic function F of a set $\gamma(F, (\Sigma_0))$ we define a piecewise reflexive recursion as follows:

$$F(n) = \begin{cases} T(lr(n)) \cdot T(rr(n)) \text{ if } 5 \leqslant l(n) \leqslant 6 \\ F(lr(n)) \cdot F(rr(n)) \text{ if } 7 \leqslant l(n) \leqslant 9 \\ F(r(n)) \text{ if } l(n) = 10 \\ F(rr(n)) \text{ if } 11 \leqslant l(n) \leqslant 12 \\ 0 \text{ otherwise.} \end{cases}$$

Consider a function Sb defined by a piecewise reflexive recursion as follows:

$$\mathrm{Sb}(n, m, k) = \begin{cases} k, \text{ if } l(n) = 1 \text{ and } r(n) = m \\ c(l(n), c(\mathrm{Sb}(lr(n), m, k), \mathrm{Sb}(rr(n), m, k))) \text{ if } 3 \leqslant l(n) \leqslant 9 \\ c(l(n), \mathrm{Sb}(r(n), m, k)) \text{ if } l(n) \in \{2, 10\} \\ c(l(n), c(lr(n), \mathrm{Sb}(rr(n), m, k))) \text{ if } 11 \leqslant l(n) \leqslant 12 \\ \qquad\qquad \text{and } m \neq lr(n) \\ n \text{ otherwise.} \end{cases}$$

It is easy to verify that if $\theta \in T(\Sigma_0) \cup F(\Sigma_0)$ and $t \in T(\Sigma_0)$, then $\mathrm{Sb}(\gamma\theta, m, \gamma t) = \gamma\theta'$, where θ' is obtained from θ by replacing all free occurrences of the variable v_m by a term t.

We define by a piecewise reflexive recursion a two-place function Fr possessing the following property: for any $\theta \in T(\Sigma_0) \cup F(\Sigma_0)$ we have $\mathrm{Fr}(\gamma\theta, n) = 1$ if v_n occurs free in θ and $\mathrm{Fr}(\gamma\theta, n) = 0$ otherwise.

$$\mathrm{Fr}(n, m) = \begin{cases} \overline{\mathrm{sg}}\,(\delta(r(n), m)) \text{ if } l(n) = 1 \\ \mathrm{Fr}(r(n), m) \text{ if } l(n) \in \{2, 10\} \\ \mathrm{sg}(\mathrm{Fr}(lr(n), m) + \mathrm{Fr}(rr(n), m)) \text{ if } 3 \leqslant l(n) \leqslant 9 \\ \mathrm{Fr}(rr(n), m) \text{ if } 11 \leqslant l(n) \leqslant 12 \text{ and } m \neq lr(n) \\ 0 \text{ otherwise.} \end{cases}$$

Consider a function P defined by a piecewise reflexive recursion as follows:

$$P(n, m, k) = \begin{cases} 1 \quad \text{if} \quad 0 \leqslant l(n) \leqslant 6 \\ P(r(n), m, k) \quad \text{if} \quad l(n) = 10 \\ P(lr(n), m, k) \cdot P(rr(n), m, k) \quad \text{if} \quad 7 \leqslant l(n) \leqslant 9 \\ P(rr(n), m, k) \quad \text{if} \quad 11 \leqslant l(n) \leqslant 12 \quad \text{and} \\ \qquad\qquad \mathrm{Fr}(rr(n), m) \cdot \mathrm{Fr}(k, lr(n)) = 0 \\ 0 \text{ otherwise.} \end{cases}$$

If $\Phi \in F(\Sigma_0)$, $t \in T(\Sigma_0)$, then $P(\gamma\Phi, m, \gamma t) = 1$ when the condition on the notation $(\Phi)_t^{vm}$ holds (see Section 18) and $P(\gamma\Phi, m, \gamma t) = 0$ otherwise.

With the recursive functions T, F, Sb, Fr and P at our disposal, it is easy to construct the recursive characteristic function A of the set of axioms of $\mathrm{CP}_1^{\Sigma_0}$. It suffices to construct a characteristic function A_i for a set of axioms obtained according to a schema i for any $i \in \{1, 2, \ldots, 12\}$. We construct A_1 and A_{11}. Constructing A_i for the other i will be left as an easy exercise to the reader.

$$A_1(n) = \begin{cases} 1 \text{ if } F(n) = 1,\ l(n) = 9,\ lrr(n) = 9 \text{ and} \\ \qquad\qquad\qquad\qquad lr(n) = rrrr(n) \\ 0 \text{ otherwise,} \end{cases}$$

$$A_{11}(n) = \begin{cases} 1 \text{ if } F(n) = 1,\ l(n) = 9,\ llr(n) = 12 \text{ and } \Phi(n) \\ 0 \text{ otherwise,} \end{cases}$$

where

$$\Phi(n) = \exists x \leqslant n(T(x) \wedge rr(n) = \mathrm{SB}(rrlr(n),$$
$$lrlr(n), x) \wedge P(rrlr(n), lrlr(n), x)). \quad \square$$

PROPOSITION 3. *A set of theorem of* $CP_1^{\Sigma_0}$ *is recursively enumerable.*

PROOF. Using functions F and Fr it is easy to construct definitions by piecewise reflexive recursion of a three-place function $\mathrm{R1}_1$ and two-place functions $\mathrm{R1}_2$, $\mathrm{R1}_3$ for which $\mathrm{R1}_1(n, k, m) = 1$, $\mathrm{R1}_2(n, m) = 1$ and $\mathrm{R1}_3(n, m) = 1$ precisely when $n = \gamma\Phi$, $m = \gamma\Psi$, $k = \gamma\Theta$ for $\Phi, \Psi, \Theta \in F(\Sigma_0)$ and Ψ is obtained from Φ, Θ or Φ by Rules 1, 2 or 3 respectively. For example,

$$\mathrm{R1}_2(n, m) = \begin{cases} 1 \text{ if } l(n) = l(m) = 9,\ lrr(m) = 12, \\ \qquad\qquad\qquad rr(n) = rrrr(m),\ F(n) = 1 \\ \qquad\qquad lr(n) = lr(m) \text{ and } \mathrm{Fr}(lr(n), lrrr(m)) = 0 \\ 0 \text{ otherwise.} \end{cases}$$

To define another very important function consider a signature Σ obtained from Σ_0 by adding to it the function symbols

l, r, β, A, $\mathrm{R1}_1$, $\mathrm{R1}_2$, $\mathrm{R1}_3$ and the corresponding algebraic system Ω_Σ, where these symbols correspond to the recursive functions on ω designated earlier by the same symbols. Let φ be a Σ-formula defined as follows:

$$\begin{aligned}\forall x \leqslant r(u)(A(\beta(l(u), x)) = \\ = 1 \vee \exists y \leqslant x \exists z \leqslant x(\neg y \approx x \wedge \neg z \approx \\ \approx x \wedge (\mathrm{R1}_1(\beta(l(u), y), \beta(l(u), z), \beta(l(u), x)) \vee \\ \vee \mathrm{R1}_2(\beta(l(u), y), \beta(l(u), x)) \vee \mathrm{R1}_3(\beta(l(u), y), \beta(l(u), x))));\end{aligned}$$

$FV(\varphi) = \{u\}$. We now define a one-place recursive function Pr as follows:

for $n \in \omega$

$$\mathrm{Pr}(n) = \begin{cases}\beta(l(n), r(n)) \text{ if } \varphi[\eta] \text{ for } \eta = \{\langle u, n\rangle\} \\ \gamma(v_0 \approx v_0) \text{ otherwise.}\end{cases}$$

It remains to verify (and this will be left for the reader to do) that the function Pr enumerates the set of theorems of $\mathrm{CP}_1^{\Sigma_0}$. □

Consider a collection Γ_0 of sentences which are universal closures of the following formulas of a signature Σ_0:

(1) $\neg s(v_0) \approx 0$,
(2) $s(v_0) \approx s(v_1) \to v_0 \approx v_1$,
(3) $v_0 + 0 \approx v_0$,
(4) $v_0 + s(v_1) \approx s(v_0 + v_1)$,
(5) $v_0 \cdot 0 \approx 0$,
(6) $v_0 \cdot s(v_1) \approx (v_0 \cdot v_1) + v_0$,
(7) $\neg v_0 < 0$,
(8) $v_0 < s(v_1) \to (v_0 < v_1 \vee v_0 \approx v_1)$,
(9) $(v_0 < v_1 \vee v_0 \approx v_1 \to v_0) < s(v_1)$,
(10) $\neg v_0 \approx v_1 \to (v_0 < v_1 \vee v_1 < v_0)$.

The set of sentences of Σ_0 derived in $\mathrm{CP}_1^{\Sigma_0}$ from the axioms Γ_0 is called a *theory* A_0. It is clear that $\Omega = \langle \omega; \underline{+}, \underline{\cdot}, \underline{<}, \underline{0}\rangle$, where $\underline{+}$, $\underline{\cdot}$, $\underline{<}$, $\underline{0}$ denote the operations of addition, and multiplication, the "less than" relation and the number 0 respectively, is the model A_0. In particular A_0 is consistent.

A term $s(s(\ldots s(0)\ldots))$, where the number of symbols s equals n, is, as in Section 36, denoted by $\underline{n}$.

DEFINITION. A function $f\colon \omega^n \to \omega$ is said *to be representable in a theory* A_0 if there is a formula $\Phi(x_1, \ldots, x_n, y)$ of Σ_0 such that for any $m_1, \ldots, m_n, m \in \omega$

$$f(m_1, \ldots, m_n) = m \Rightarrow A_0 \rhd \Phi(\underline{m_1}, \ldots, \underline{m_n}, \underline{m}), \tag{1}$$

$$f(m_1, \ldots, m_n) \neq m \Rightarrow A_0 \rhd \neg\Phi(\underline{m_1}, \ldots, \underline{m_n}, \underline{m}). \tag{2}$$

If for an n-place function f and a formula $\Phi(x_1, \ldots, x_n, y)$ (1) and (2) hold for all $m, m_1, \ldots, m_n \in \omega$, then $\Phi(x_1, \ldots, x_n, y)$ *is said to represent in* A_0 *the function* f. Note that this relation depends not only on the formula Φ and the function f but also on the ordering of the variables $x_1, \ldots, x_n, y$. A formula Φ will be said to represent an n-place function f if $\Phi(x_1, \ldots, x_n, y)$ represents f for some variables $x_1, \ldots, x_n; y$.

LEMMA 1. *Let* $n, m \in \omega$. *Then*

(a) $A_0 \rhd x < s(\underline{n}) \to (x \approx \underline{0} \vee \ldots \vee x \approx \underline{n})$;

(b) *if* $n \neq m$, *then* $A_0 \rhd \neg \underline{n} \approx \underline{m}$;

(c) *if* $n < m$, *then* $A_0 \rhd \underline{n} < \underline{m}$;

(d) *if* $n \leqslant m$, *then* $A_0 \rhd \neg \underline{m} - \underline{n}$.

PROOF. If $n = 0$, then (a) follows from axioms (7) and (8). For $n = k + 1$ (a) follows from the truth of (a) for k and from axiom (8). Statement (b) for $m = \underline{0}$ follows from axiom (1). Suppose statement (b) for $m \leqslant k$ is proved and let $n \neq k + 1$. If $n = 0$, then (b) follows from axiom (1). If $n = l + 1$, then $l \neq k$ and under the hypothesis $A_0 \rhd \neg \underline{l} \approx \underline{k}$. From axiom (2) we then get $A_0 \rhd \neg \underline{n} \approx \underline{k+1}$.

Statement (c) will be proved by induction on m. If $m = 0$, then there is nothing to prove. If $m = k + 1$, then $n < k$ or $n = k$ and by the induction hypothesis $A_0 \rhd \underline{n} < \underline{k} \vee \underline{n} \approx \underline{k}$. From axiom (9) we now get $A_0 \rhd \underline{n} < \underline{m}$.

Statement (d) will be proved by induction on n. When $n = 0$ (d) is axiom (7). If $k + 1 \leqslant m$, then by the induction hypothesis and (b) we get $A_0 \rhd \neg \underline{m} < \underline{k} \wedge \neg \underline{m} \approx \underline{k}$. From axiom (8) we then get $A_0 \rhd \neg \underline{m} < \underline{k+1}$. □

LEMMA 2. Formulas $v_0 + v_1 \approx v_2$ *and* $v_0 \cdot v_1 \approx v_2$ *represent in* A_0 *the functions of addition and multiplication respectively.*

PROOF. We show that the formula $\underline{m} + \underline{n} \approx \underline{m+n}$ belongs to the theory A_0 by induction on n. For $n = 0$ this is axiom (3). The induction step follows from axiom (4). Condition (2) now follows from Lemma 1(b). Verification for multiplication will be left to the reader. □

THEOREM 5. *Any recursive function is representable in A_0.*

PROOF. By virtue of Theorem 36.3 it suffices to construct for any recursive formula φ, $FV(\varphi) \subseteq \{x_1, \ldots, x_n\}$, and any recursive term t, $FV(t) \subseteq \{x_1, \ldots, x_n\}$, formulas $\Phi_\varphi(x_1, \ldots, x_n)$, $\Psi_t(x_1, \ldots, x_n, y)$ of Σ_0 such that for any $m_1, \ldots, m_n, m \in \omega$ the following conditions hold:

$$\langle m_1, \ldots, m_n \rangle \in \varphi[x_1, \ldots, x_n] \Rightarrow A_0 \rhd \Phi_\varphi(\underline{m_1}, \ldots, \underline{m_n}), \tag{3}$$

$$\langle m_1, \ldots, m_n \rangle \notin \varphi[x_1, \ldots, x_n] \Rightarrow A_0 \rhd \neg\Phi_\varphi(\underline{m_1}, \ldots, \underline{m_n}), \tag{4}$$

$$t[x_1, \ldots, x_n](m_1, \ldots, m_n) = m \Rightarrow A_0 \rhd \Psi_t(\underline{m_1}, \ldots, \underline{m_n}, m), \tag{5}$$

$$A_0 \rhd (\Psi_t(m_1, \ldots, m_n, y) \wedge \Psi_t(\underline{m_1}, \ldots, \underline{m_n}, z) \rightarrow y \approx z). \tag{6}$$

We simultaneously construct Φ_φ and Ψ_t by induction on the length of φ and t:

(a) $\Psi_0 = y \approx 0$,
(b) $\Psi_x = y \approx x$,
(c) $\Psi_{s(t)} = \exists z((\Psi_t)^y_z \wedge y \approx s(z))$,
(d) $\Psi_{t\tau q} = \exists z \exists w((\Psi_t)^y_z \wedge (\Psi_t)^y_w \wedge y \approx z\tau w)$, $\tau \in \{+, \cdot\}$,
(e) $\Phi_{t\tau q} = \exists z \exists w((\Psi_t)^y_z \wedge (\Psi_q)^y_w \wedge z\tau w)$, $\tau \in \{\approx, <\}$,
(f) $\Phi_{\neg\varphi} = \neg\Phi_\varphi$,
(g) $\Phi_{(\varphi\tau\Psi)} = (\Phi_\varphi \tau \Phi_\Psi)$, $\tau \in \{\wedge, \vee, \rightarrow\}$,
(h) $\Psi_{\mu x\varphi} = (\Phi_\varphi)^x_\mu \wedge \forall x(x < y \rightarrow \neg\Phi_\varphi)$.

We must now establish in each of the cases (a) to (h) of the definition of formulas Φ_φ, Ψ_t the validity of (3), (4) or (5), (6) respectively. Cases (a) to (c) and (e) follow from the induction hypothesis and Lemma 1. Case (d) follows from Lemma 2 and the induction hypothesis. Cases (f) and (g) are obvious. Let us verify (h). Since $\mu x\varphi$ is a recursive term, $FV(\mu x\varphi) \subseteq \{x_1, \ldots, x_n\}$, given any $m_1, \ldots, m_n \in \omega$ there is $m \in \omega$ such that $\varphi[\eta]$ for any $\eta = \{\langle x_i, m_i\rangle \mid i = 1, \ldots, n\} \cup \{\langle x, m\rangle\}$. From axiom (10) we obtain the truth of (6). From the induction hypothesis and Lemma 1(a) we obtain the truth of (5). □

THEOREM 6. *If T is a consistent theory of Σ_0 and $A_0 \subseteq T$, then the set $X_T = \{\gamma(\Phi) \mid \Phi \in F(\Sigma_0),\ T \rhd \Phi\}$ is nonrecursive.*

PROOF. Consider a one-place function Nm defined by the following schema:

$$\begin{aligned} \mathrm{Nm}(0) &= c(0,\ 1), \\ \mathrm{Nm}(n+1) &= c(2,\ \mathrm{Nm}(n)). \end{aligned}$$

It is clear that Nm is a recursive function and that for any n $\mathrm{Nm}(n) = \gamma(\underline{n})$. We denote by $\mathrm{Sb}_0(x, y)$ a function $\mathrm{Sb}(x, 0, \mathrm{Nm}(y))$ (Sb is defined in the proof of Proposition 2). Notice that if $\Phi \in F(\Sigma_0)$, $n \in \omega$, then $\mathrm{Sb}_0(\gamma(\Phi), n) = \gamma(\Psi)$, where Ψ is obtained from Φ by replacing all free occurrences of the variable v_0 by the term $\underline{n}$.

Suppose that there is a recursive characteristic function of X_T. By the preceding theorem there is a formula $\Phi(x, y, z)$ representing in A_0 a function $f(\mathrm{Sb}_0)$. On replacing, if necessary, the formula Φ by a congruent formula it may be assumed that Φ contains no bound variable v_0. Let $n_0 = \gamma((\neg\Phi)^{x,\,y,\,z}_{v_0,\,v_0,\,\underline{1}})$. If $f(\mathrm{Sb}_0(n_0, n_0)) = 1$, then $\gamma(\neg\Phi(\underline{n_0}, \underline{n_0}, \underline{1})) \in X_T$ and therefore $T \rhd \neg\Phi(\underline{n_0}, \underline{n_0}, 1)$. But this is impossible by virtue of the fact that $f(\mathrm{Sb}_0)$ is representable in $A_0 \subseteq T$ by a formula $\Phi(x, y, z)$ and the consistency of T. Thus $f(\mathrm{Sb}_0(n_0, n_0)) = 0$. From the fact that $\Phi(x, y, z)$ represents in A a function $f(\mathrm{Sb}_0)$ and from the inclusion $A_0 \subseteq T$ we get $T \rhd \neg\Phi(\underline{n_0}, \underline{n_0}, \underline{1})$. Hence $\gamma(\neg\Phi(\underline{n_0}, \underline{n_0}, \underline{1})) \in X_T$ and $f(\mathrm{Sb}_0(n_0, n_0)) = 1$, a contradiction. □

COROLLARY 1 (Church). *The set of theorems of* $\mathrm{CP}_1^{\Sigma_0}$ *is nonrecursive.*

PROOF. Suppose Φ_0 is a conjunction of axioms (1) to (10) of a theory A_0 and $\Phi_1 = \forall v_0 \forall v_1 \forall v_2 \Phi_0$. It is clear that for any formula Ψ of Σ_0 we have

$$A_0 \rhd \Psi \Leftrightarrow (\Phi_1 \rightarrow \Psi \text{ is a theorem of } \mathrm{CP}_1^{\Sigma_0}). \qquad (7)$$

Let the characteristic function f of a set $X_0 = \{\gamma(\Phi) \mid \Phi$ is a theorem of $\mathrm{CP}_1^{\Omega_0}\}$ be recursive. Then so is a function $g = f(c(9, c(n_0, x)))$, where $n_0 = \gamma(\Phi_1)$. By (7) g is the characteristic function of a set $\{\gamma(\Phi) \mid \Phi \in F(\Sigma_0), A_0 \rhd \Phi\}$ and by Theorem 6 it cannot be recursive, a contradiction. □

From Proposition 3 and Corollary 1 we get

COROLLARY 2. *There is a recursively enumerable nonrecursive set.* □

A theory T of Σ_0 is said to be *axiomatizable* if there is a recursively enumerable set Γ of axioms for T.

LEMMA 3. *If T is an axiomatizable theory of a signature Σ_0, then the set $X_T = \{\gamma(\Phi) \mid \Phi \in F(\Sigma_0), T \rhd \Phi\}$ is recursively enumerable.*

PROOF. Let f be a recursive function enumerating a set $\gamma[\Gamma]$, where Γ is the set of axioms for T. Let Pr be the function of Proposition 3 enumerating the theorems of $\mathrm{CP}_1^{\Sigma_0}$. Consider a function g defined as follows:

$$g(0) = f(0)$$

$$g(n+1) = c(7, c(g(n), f(n+1))).$$

Let $f(i) = \gamma(\Phi_i)$, $i \in \omega$. Then $g(n) = \gamma(\ldots(\Phi_0 \wedge \Phi_1) \wedge \ldots \wedge \Phi_n)$ and

$$X_T = \{\Phi \mid \Phi \in F(\Sigma_0), \rhd (\Phi_0 \wedge \ldots \wedge \Phi_n) \rightarrow \Phi, n \in \omega\}.$$

Consequently the function Pr_T defined by the schema

$$\mathrm{Pr}_T(n) = \begin{cases} rr(Pr(l(n))) \text{ if } l(\mathrm{Pr}(l(n))) = 9 \\ \qquad\qquad\qquad\qquad \text{and } lr(\mathrm{Pr}(l(n))) = g(r(n)) \\ \gamma(v_0 \approx v_0) \text{ otherwise} \end{cases}$$

will enumerate the set X_T. □

Recall that a theory T of Σ is said *to be complete* if it is consistent and for any closed formula Φ of Σ either $\Phi \in T$ or $\neg\Phi \in T$.

LEMMA 4. *If a theory T of Σ_0 is axiomatizable and complete, then the set $X_T = \{\gamma(\Phi) \mid \Phi \in F(\Sigma_0), T \rhd \Phi\}$ is recursive.*

PROOF. Consider a two-place function f defined as follows:

$$f(m, 0) = c(12, c(0, m)),$$

$$f(m, n+1) = c(12, c(n+1, f(m, n))).$$

For $\Phi \in F(\Sigma_0)$ we then have $f(\gamma(\Phi), n] = \gamma(\forall v_n \forall v_{n-1} \cdots \forall v_0 \Phi)$. Since $c(k, s) \geqslant k, s$, the subscripts of the variables occurring in Φ do not exceed $\gamma(\Phi)$. Hence a formula Ψ for which $\gamma(\Psi) = f(\gamma(\Phi), \gamma(\Phi))$ is closed for any $\Phi \in F(\Sigma_0)$. Notice that for any $\Phi \in F(\Sigma_0)$ we have

$$T \rhd \Phi \Leftrightarrow T \rhd \Psi,$$

where $\gamma(\Psi) = f(\gamma(\Phi), \gamma(\Phi))$. Let Pr_T be the function of Lemma 3 enumerating the set X_T. The completeness of T yields $n \notin X_T \Leftrightarrow$ $\Leftrightarrow (F(n) = 0$ or $c(10, f(n, n)) \in X_T)$, where F is the characteristic function of a set $F(\Sigma_0)$. Therefore the function g defined as follows:

$$g(n) = \begin{cases} l(n) \text{ if } \mathrm{Pr}_T(r(n)) = c(10, f(l(n), l(n))) \text{ or } F(l(n)) = 0 \\ \gamma(\neg v_0 \approx v_0) \text{ otherwise} \end{cases}$$

will enumerate a set $\omega \setminus X_T$. From Proposition 37.1 we see that X_T is recursive. □

THEOREM 7 (Gödel's Incompleteness Theorem). *Any axiomatizable theory T of Σ_0 which is an extension of A_0 is incomplete.*

PROOF. Immediate from Theorem 6 and Lemma 4. □

Gödel's incompleteness theorem is of the utmost importance for the foundations of mathematics. While from Theorem 6 and Church's thesis it follows that there is no universal method for proving the theorems of arithmetic, from Gödel's incompleteness theorem and Church's thesis we see that there is even no effective way of giving the axioms of arithmetic. (By arithmetic we mean here the theory of the system $\Omega = \langle \omega; \pm, \dot{-}, \leqslant, 0 \rangle$.)

In conclusion we prove, as promised in Section 37, the existence of recursively enumerable predicates.

THEOREM 8. *For any $n \neq 0 \in \omega$ there is an $(n + 1)$-place recursively enumerable predicate universal for the family of all n-place recursively enumerable predicates.*

PROOF. Consider an $(n + 1)$-place predicate R defined as follows: for any $m_0, m_1, \ldots, m_n \in \omega$

$$\langle m_0, m_1, \ldots, m_n \rangle \in R \Leftrightarrow m_0 \text{ is a Gödel number of some formula } \Phi \text{ of } \Sigma_0 \text{ and } A_0 \rhd (\Phi)^{v_0, \ldots, v_{n-1}}_{m_1, \ldots, m_n}.$$

Using the function constructed above it is easy to define an $(n+1)$-place recursive function f such that for any $m_0, \ldots, m_n \in \omega$

(a) if $F(m_0) = 0$, i. e. m_0 is not a Gödel number of some formula, then $f(m_0, \ldots, m_n) = \gamma(\neg \underline{0} \approx \underline{0})$;

(b) if $F(m_0) = 1$ and Φ is a formula such that $\gamma(\Phi) = m_0$, then

$$f(m_0, m_1, \ldots, m_n \rangle = \gamma(\Phi_1 \rightarrow (\Phi)^{v_0, \ldots, v_{n-1}}_{m_1, \ldots, m_n}),$$

where Φ_1 is the sentence defined in the proof of Corollary 1 of Theorem 6.

If X_0 is a set of Gödel numbers of theorems of $CP_1^{\Sigma_0}$, then we see from the definition of a function f that the following relation is true: for any $m_0, m_1, \ldots, m_n \in \omega$

$$\langle m_0, m_1, \ldots, m_n \rangle \in R \Leftrightarrow f(m_0, m_1, \ldots, m_n) \in X_0.$$

Thus the predicate R is m-reducible to the set X_0. By Proposition 3 X_0 is recursively enumerable. Hence by Proposition 37.2 R is also recursively enumerable.

We show that it is R that is universal for the family of all n-place recursively enumerable predicates.

Suppose R^0 is an n-place recursively enumerable predicate and φ is a recursive formula such that $FV(\varphi) \subseteq \{v_0, \ldots, v_n\}$ and

$$R^0 = (\exists v_n \varphi)[v_0, \ldots, v_{n-1}].$$

If $\Phi_\varphi(v_0, \ldots, v_n)$ is the formula in the proof of Theorem 5, then for any $m_0, \ldots, m_{n-1}, m_n \in \omega$ the following holds:

$$\langle m_0, \ldots, m_{n-1}, m_n \rangle \in \varphi[v_0, \ldots, v_n] \Rightarrow$$
$$\Rightarrow A_0 \rhd \Phi_\varphi(\underline{m_0}, \ldots, \underline{m_{n-1}}, \underline{m_n}),$$

$$\langle m_0, \ldots, m_{n-1}, m_n \rangle \notin \varphi[v_0, \ldots, v_n] \Rightarrow$$
$$\Rightarrow A_0 \rhd \neg \Phi_\varphi(\underline{m_0}, \ldots, \underline{m_{n-1}}, \underline{m_n}).$$

We consider the formula $\Phi(v_0, \ldots, v_{n-1}) = \exists v_n \Phi_\varphi(v_0, \ldots, v_{n-1}, v_n)$ and prove the following relation: for any $m_0, \ldots, m_{n-1} \in \omega$ $\langle m_0, \ldots, m_{n-1} \rangle \in R^0 \Leftrightarrow$

$$\Leftrightarrow A_0 \rhd (\Phi)^{v_0, \ldots, v_{n-1}}_{\underline{m_0}, \ldots, \underline{m_{n-1}}} \; (= \Phi(\underline{m_0}, \ldots, \underline{m_{n-1}})).$$

Indeed, if $\langle m_0, \ldots, m_{n-1} \rangle \in R^0$, then for some $m_n \in \omega$ $\langle m_0, \ldots, m_{n-1}, m_n \rangle \in \varphi[v_0, \ldots, v_n]$. Hence $A_0 \rhd \Phi_\varphi(\underline{m_0}, \ldots, \underline{m_{n-1}}, \underline{m_n})$ and

$$A_0 \rhd \Phi(\underline{m_0}, \ldots, \underline{m_{n-1}})(= \exists v_n \Phi_\varphi(\underline{m_0}, \ldots, \underline{m_{n-1}}, v_n)).$$

Conversely, let $A_0 \rhd \Phi(\underline{m_0}, \ldots, \underline{m_{n-1}})$. Then $\Omega \vDash \exists v_n \Phi_\varphi(\underline{m_0}, \ldots, \underline{m_{n-1}}, v_n)$ since Ω is a model of A_0. Therefore for some $m_n \in \omega$ $\Omega \vDash \Phi_\varphi(\underline{m_0}, \ldots, \underline{m_{n-1}}, \underline{m_n})$. We now show that $\langle m_0, \ldots, m_{n-1}, m_n \rangle \in \varphi[v_0, \ldots, v_n]$. Indeed, if this were not the case, then $A_0 \rhd \neg \Phi_\varphi(\underline{m_0}, \ldots, \underline{m_{n-1}}, \underline{m_n})$ and hence $\Omega \vDash \neg \Phi_\varphi(\underline{m_0}, \ldots, \underline{m_{n-1}}, \underline{m_n})$. So $\langle m_0, \ldots, m_{n-1}, m_n \rangle \in \varphi[v_0, \ldots, v_n]$ and hence $\langle m_0, \ldots, m_{n-1} \rangle \in R^0$. Let $k = \gamma(\Phi)$. Then from the foregoing we have

for any $m_0, \ldots, m_{n-1} \in \omega$

$$\langle k, m_0, \ldots, m_{n-1} \rangle \in R \Leftrightarrow A_0 \rhd (\Phi)^{v_0, \ldots, v_{n-1}}_{\underline{m_0}, \ldots, \underline{m_{n-1}}} \Leftrightarrow$$

$$\Leftrightarrow \langle m_0, \ldots, m_{n-1} \rangle \in R^0.$$

Thus $R^0 = R_k$. □

COROLLARY 1. *For any $n \in \omega$, $n \neq 0$, there is an $(n + 1)$-place partially recursive function universal for the family of all n-place partially recursive functions.*

This follows from the theorem and Proposition 37.6. □

In the course of the proof the following fact was in essence also established.

COROLLARY 2. *The set X_0 of Gödel numbers of the theorems of* $\mathrm{CP}_1^{\Sigma_0}$ *is an m-universal recursively enumerable set.* □

Exercises

1. Suppose T is a theory of Σ, $\Phi_0(x, w_1, \ldots, w_s)$, $\Phi_1(x, y, z, w_1, \ldots, w_n)$, $\Phi_2(x, y, z, w_1, \ldots, w_m) \in F(\Sigma)$. Show that if there is a model $\mathfrak{A}$ of T, elements $c_1, \ldots, c_s$, $a_1, \ldots, a_n, b_1, \ldots, b_m \in A$ and a mapping $f\colon \omega \to A$ for which the following conditions hold:

(a) $f[\omega] = \{a \mid \mathfrak{A} \models \Phi_0(a, c_1, \ldots, c_s)\}$,

(b) $k + l = r \Leftrightarrow \mathfrak{A} \models \Phi_1(fk, fl, fr, a_1, \ldots, a_n)$,

(c) $k \cdot l = r \Leftrightarrow \mathfrak{A} \models \Phi_2(fk, fl, fr, b_1, \ldots, b_m)$,

then the theory T is undecidable, i. e. the set $X_T = \{\Phi \in F(\Sigma) \mid T \rhd \Phi\}$ is nonrecursive. (*Hint.* Apply Theorem 6.)

2. Using Exercise 1 prove that the sets of theorems of CP^{Σ_1} and CP^{Σ_2}, where $\Sigma_1 = \langle f^2 \rangle$ and $\Sigma_2 = \langle r^2 \rangle$ contain one two-place function symbol and one two-place predicate symbol respectively, are nonrecursive and that hence CP^{Σ} is undecidable for any signature Σ containing not only one-place symbols.

List of Symbols

$\Rightarrow$, $\Leftrightarrow$, $\square$ 8
$\subseteq$ 15
$=$ 15
$\in$ 15
$\varnothing$ 16
$\{a_1, \ldots, a_n\}$ 16, 65
$\{a \mid \varphi(a)\}$ 16
Λ 16
$\alpha * \beta$ 17
$\langle X_1, \ldots, X_n \rangle$ 18
$X_1 \times \ldots \times X_n$ 18
$f(a)$ 18, 69
$f: X \to Y$ 18, 69
$\cap$, $\cup$, $\setminus$ 19
$\bigcup_{i \in I} X_i$ 20
$P(X)$ 20
$X_0, \ldots, X_n \to Y$ 20
Q_i 22
$\wedge$, $\vee$, $\to$, $\neg$, $\vdash$ 22
(,) 22
PC 22
$\Phi \equiv \psi$ 34, 126
$D(\Phi)$, $K(\Phi)$ 38
$\bigwedge_{i=1}^{n} \Phi_i$, $\bigvee_{i=1}^{n} \Phi_i$ 39
$\Phi_1 \wedge \ldots \wedge \Phi_n$,
  $\Phi_1 \vee \ldots \vee \Phi_n$ 39
$f_X(\Phi)$ 43
$T_\Phi(P_c, \ldots, P_k)$ 45
PC_1 52
$\triangleright$ 52, 140
$I_0 < I_1$ 56
$PC^{(\to)}$ 57
$PC^{(\to, \vee)}$ 58
π_i^n 66
$\langle a, b \rangle$ 66
ω 65
B^{-1} 66
id_A 67
(BC), $B \cdot C$ 67
E_R, R_E 68
dom f, rang f 68
$f[A]$ 69
$f \restriction A$ 69
$f: A \twoheadrightarrow B$ 69
sup $(A_1, \mathfrak{A})$ 70
inf $(A_1, \mathfrak{A})$ 71
$\cup^{\mathfrak{A}}$, $\cap^{\mathfrak{A}}$ 71
$0^{\mathfrak{A}}$, $1^{\mathfrak{A}}$ 71
$O[a_0, \mathfrak{A}]$, $O(a_0, \mathfrak{A})$ 74
$|A| \leqslant |B|$ 82
$|A| = |B|$ 83

$\varepsilon(X)$ 84
$\alpha + 1$ 84
$\bigcup X$ 85
$|X|$ 87
V_α 90
$\rho(X)$ 90
ZF, ZFC 92
$\Sigma = \langle R, F, \mu \rangle$ 96
$\mathfrak{A} = \langle A, \nu^{\mathfrak{A}} \rangle$ 97
$\bigcup_{n \in \omega} \Sigma_n$, $|\Sigma|$ 97
$f\colon \mathfrak{A} \simeq \mathfrak{B}$, $\mathfrak{A} \simeq \mathfrak{B}$ 97
$\mathfrak{B}(X)$, $\mathfrak{B}(a_1, \ldots, a_n)$ 98
$\bigcup_{i \in I} \mathfrak{A}_i$ 99
$T(\Sigma)$ 102
$V = \{v_i \mid i \in \omega\}$ 103
$FV(t)$ 103, 251
$t^{\mathfrak{A}}[\gamma]$ 103
$F(\Sigma)$, $\approx$ 104
$\forall$, $\exists$ 104
$FV(\Phi)$ 105
$\mathfrak{A} \models \Phi[\gamma]$ 106
I-prod X_i 111
$f \overset{D}{\sim} g$ 111
D-prod X_i, D-prod $\mathfrak{A}_i$ 111
I-prod $\mathfrak{A}_i$ 112
CP^{Σ} 117
$(\Phi)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$; $[\Phi]^x_y$ 117
$\Phi \overset{s}{\equiv} \Psi$ 126
$\Phi \sim \Psi$ 129
CP^{Σ}_1 139
$\Phi \overset{1}{\equiv} \Psi$ 141

CPP 144
Σ^* 144
$\alpha * \Phi$, $\alpha_0 \Phi$ 145
Th $(\mathfrak{A})$ 149
$\mathfrak{A} \equiv \mathfrak{B}$ 149
$\mathfrak{A} < \mathfrak{B}$ 153
C_X, Σ_X, $\mathfrak{A}_X$ 155
$D(\mathfrak{A}, X)$, $D^*(\mathfrak{A}, X)$ 155
$D(\mathfrak{A})$, $D^*(\mathfrak{A})$ 155
$K_\Sigma(Z)$ 157
Th (K) 157
E_Σ 162
$\Phi \overset{T}{\equiv} \Psi$ 165
Σ^s, T^s, $\mathfrak{A}^s$ 166
Σ^{cs}, T^{cs}, $\mathfrak{A}^{cs}$ 167
$\Phi^{\urcorner}$ 168
Σ^c 168
$\mathfrak{A}/E$ 177
$\|\Phi\|$ 181
K_+, K_∞ 191
G 198
$I^n(I)$ 199
$F_x(t)$ 217
$GS(\Phi)$ 239
$R_P(\Gamma_0; \ldots; \Gamma_n)$ 228
$R(\Gamma_0; \ldots; \Gamma_n)$ 232
$\mathfrak{A}(a)$ 236
$\mathfrak{A}\colon \alpha \vdash \beta$, $\mathfrak{A}\colon \alpha \vdash \cdot \beta$ 239
$\mathfrak{A}\colon \alpha \models \beta$, $\mathfrak{A}\colon \alpha \models \cdot \beta$ 239
α^a, α_a 244
$\alpha \xrightarrow{M} \beta$ 244
$\mathfrak{F}_n$, $\mathfrak{F}$ 248
$S^{k, n}$, R^n 248

M^n 249
o, s, I^n_m 249
$+, \cdot, \dot{-}$ 250
sg, $\overline{\text{sg}}$ 250
Σ_0 251
$FV(\varphi)$ 252
π_X 254
χ_X 254
$\mu x \leqslant t\varphi$ 258
$\exists x \leqslant t\varphi, \forall x \leqslant t\varphi$ 258
$\leqslant, [/]$ 259
$[\sqrt{\ }]$, rest 259
c, l, r 259
β 260
Γ_f 265
$\leqslant m$ 275
γ 277
$T(\Sigma_0), F(\Sigma_0), A(\Sigma_0)$ 280
A_n, Rl_n 282
Pr 283
A_0 283

Subject Index

Algebraic system, 97
  canonical, 170
  homogeneous, 181
  recursive, 254
  saturated, 184
  universal, 184
  $\varkappa$-saturated, 187
Algebraic systems, elementarily equivalent, 149
Algorithm, 12, 248
  over an alphabet, 238
Algorithms, equivalent, 238
Alphabet, 16
  of the propositional calculus, 22
  of the Turing machine, exterior, 244
    interior, 244
Ancestor, 200
Application of a rule of inference, 27
Ariness mapping, 96
Arithmetic, 99
Associativity, 19
Atom of Boolean algebra, 81
Automorphism, 97
Axiom, 26
  of choice, 74
  of CP^{Σ}, 117
  of CP_1^{Σ}, 139
  of CPP, 144
  of extensionality, 65
  of PC, 26
  of PC_1, 52
  of regularity, 90
  of the calculus, 18
  of the calculus *G*, 198
Axiom schema, 26, 50
  independent, 50
Axiom system for a theory, 165

Base of tautology, 119
Basis for a system, 195
Basis function, 249
Basis term, 168
Beginning of a word, 17

Boolean algebra, 73
  of all subsets, 73
Bound occurrence of a variable, 106

Calculus, 18
  complete for the semantics, 49
  consistent, 43
    with respect to the semantics, 49
  decidable, 276
  G, 198
  G_0, 60
  independent, 50
  of predicates of Σ (CP^{Σ}), 117
  of resolvents, 228, 231
    propositional, 228
  propositional (PC), 22
  solvable, 50
  undecidable, 50
Cantor-Bernstein theorem, 83
Cantor's theorem, 83
Cardinal, 86
Carrier of an algebraic system, 97
Cartesian product, 66
  of algebraic systems, 112
Chain, 74
Characterization of PC theorems, deductive, 48
  semantic, 48
Church's thesis, 249
Class, 112
  of algebraic systems, axiomatizable, 157
    categorical, 188
    finitely axiomatizable, 159
    $\forall$-axiomatizable, 159
    $\forall\exists$-axiomatizable, 159
    $\exists$-axiomatizable, 159
Commutativity, 19
Compactness theorem, 115, 139
Complement of an element, 71
Complete theory, 165
Composition of normal algorithms, 240
  of relations, 67
Conclusion of a rule, 19
Congruence, 177
Conjunction, 22
Conjunctive normal form (cnf), 40
Conjunctive term of a formula, 37
Connective, logical, 22
Conservative extension, 56
Constant, 69
CP^{Σ} theorem, 119
Cut elimination theorem, 210

Deduction theorem, 141
Descendant, 200

Determining sequence of a partially recursive function, 249
Derivation in CP_1^Σ, 140
  in PC_1, 52
Diagonal, 67
Diagram of a set in a system, 155
  complete, 155
  of an algebraic system, 155
    complete, 155
Difference of sets, 19
Direct product of algebraic systems, 112
Disjunction, 22
Disjunctive normal form (dnf), 40
Disjunctive term of a formula, 37
Distributivity, 20
Domain of a function, 68
  of definition of an operation, 18

Empty word, 16
Equality symbol, 105
Equipotent sets, 83
Equivalence class, 68
Existential quantifier, 105
Expansion of an algebraic system, 99
Expression of a calculus, 18
  provable, 19
Extension of calculi, conservative, 56
  of a language, 19

Factor system, 177
Family set with finite intersection property, 79
Filter, countably complete, 187
  of a Boolean algebra, 79
  on a set, 79
Filtered product, 111
Formula, 22, 104, 117
  atomic 22, 104
  atomical, 104
  closed, 107
    conditionally filtering, 113
  CP^Σ-provable, 118
  filtering, 113
  identically true, 107
  in dnf, 40, 130
  in prenex nf, 130
  in reduced nf, 131
  of CP^Σ, 117
  of CPP, 144
  of PC, 22
    elementary, 22
    false on a set, 45
    identically false, 45
    identically true, 45
    true on a set, 45
  of the calculus G, 198
  of the calculus of resolvents, 228, 231
  of the signature Σ, 102
  PC-provable, 27
  positive, 178
  recursively enumerable, 264

Formula (cont.)
  satisfiable, 108
  valid, 107
Formulas, congruent, 129
  equivalent, 34, 126
    with respect to a theory T, 165
  propositionally equivalent, 126
Free occurrence of a variable, 106
Free variable of a formula, 105
Function, 68
  characteristic, 254
  completely defined, 247
  nowhere defined, 247
  partial; 243
    normally computable, 243
    Turing computable, 245
  recursive, 249
  reducing, 275
  representable in a theory A_0, 284
  representing, 254
  universal, 274
Function signature, 97

Gödel numbering, 276
Gödel's incompleteness theorem, 288
  completeness theorem, 136
Graph, 100
  of a function, 265
Greatest element, 70
Greatest lower bound (glb), 71
Group, 100
  Abelian, 100
  of substitutions, 100

Height of a sequence in a tree, 28
  of a tree, 28
Herbrand theorem, 227
Hilbertian calculus of predicates (CP_1^Σ), 139
Hilbertian propositional calculus (PC_1), 52
Homomorphism, 97
Hypothesis of a rule, 19

Idempotency, 20
Identity, 162
Image of a set under mapping, 69
Implication, 22
Initial segment, 74
  closed, 74
  open, 74
Instance of a rule of inference, 25
  of a schema, 25
Integer ring, 100
Interpolation theorem, 174
Interpretation of PC_1 in X, 43
  principal, 44
  of variables, 103
  of a signature, 97
Intersection of sets, 19, 20

k-cut of a predicate, 273

Lattice, 71
  Boolean, 71
  distributive, 71
Least element, 70
Least upper bound (lub), 70
Length of an abstract word, 17
  of a concrete word, 16
  of a sequence, 17
Letter, 15
  abstract, 15
  concrete, 15
  of an alphabet, 16
Liar paradox, 14
Limit ordinal, 85
Linear ordering, 70
Linearly ordered set, 70
List of formulas, 228
Los'theorem, 114
Lower bound, 70

Machine word, 244
Mapping, 18, 68
  distinct-valued, 68
  into, 68
  onto, 68
Matrix, 130
Maximal element, 70
Maximum principle, 75
Mechanism of compatibility, 169
  without equality, 172
Metalanguage, 34
Method, modern axiomatic, 11
Minimization operator, 249
Model, 115
Model theory, 13
Model-complete theory, 165

Natural number, 65
Negation, 22
No-go word, 245
Normal algorithm, 239
Normalization principle, 242
n-type, 173
  principal, 173
Number of places in an operation, 18
Numbering of a set, 87

Occurrence, 17
  of a letter, 17
    in a word, 17
    first, 17
    last, 17
  of a sequence, 28
    in a tree, 28
    initial, 28
Operation, 18, 68
  n-place, 18, 68
  partial, 18

Operation symbol, 96

Operator of regular superposition, 248

Ordinal, 84

Ordered collection, 65

Pair, 18

Partial ordering, 70

Partially ordered set, 70
  well-founded, 73

Partition of a set, 68

Passage in a tree, 28
  essential, 61

Place mapping, 96

Power of an algebraic system, 97
  of a set, 87
  of a signature, 97

Power set, 20

Predicate, 66
  n-place, 66
  recursive, 254
  recursively enumerable, 265
  universal, 274

Predicate signature, 97

Predicate symbol, 96

Primitive recursion operator, 248

Principal cnf, 41
  dnf, 41

Principal formula of a rule of inference, 199

Principle of potential realizability, 236
  of well ordering, 75

Problem of solvability of calculus, 49

Product of relations, 67

Programme of a Turing machine, 244

Proof, 12
  in CP^{Σ}, linear, 118
  in CP_1^{Σ}, 140
  in PC, linear, 27
  in PC_1, 52
  tree form in CP^{Σ}, 119
  tree form in PC, 28
  in the calculus of resolvents, 229

Proof theory, 13

Proof tree in CP^{Σ}, 119

Property of the purity of a variable, 201

Proposition in the English language, 21

Pure calculus of predicates, 144

Quadruple, 66

Quantifier prefix, 130

Quasi-derivation in PC, 31

Quasi-identity, 162

Quasi-variety, 162

Range of a function, 68

Rank of a set, 90

Reduction theorem, 272
Refinement, 27
Relation, 66
  antisymmetric, 67
  inverse, 66
  n-place, 66
  reflexive, 67
  symmetric, 67
  transitive, 67
Relation symbol, 96
Replacement of bound variable, 128
Replacement theorem, 35, 128
Representative of an abstract word, 16
Restriction of a relation, 67
  of a mapping, 69
  of an algebraic system, 99
Rule of inference, 18
  CP_1^Σ-admissible, 141
  in CP_1^Σ, 140
  in PC_1, 52
  independent, 50
  n-hypothesis, 19
  of CP^Σ, 117
  of PC, 26
    basic, 27
    structural, 27
  of the calculus G, 198
  of the calculus of resolvents, 228, 231
  PC-admissible, 29
Russell paradox, 9
Schema, in an alphabet, 238
  of PC formulas, 25
  of PC sequents, 25
  PC-provable, 29
Scope of a quantifier, 105
Semantic study of formal languages, 13
Semantics of a calculus, 44
Sentence, 107
  n-valid, 108
Sequence, 17
  empty, 18
Sequent, 24, 117
  of CP^Σ, 117
    true for interpretation, 122
    identically true, 122
  of CPP, 144
  CP^Σ-provable, 119
  of PC, 24
    false on a set, 46
    identically true, 46
    true on a set, 45
  of the calculus G, 198
  of the calculus G_0, 61
  PC-provable, 27
  provable in the calculus of predicates, 125
Set, 15, 65
  atomically minimal, 195
  closed under an operation, 69
  countable, 87
  defined by induction, 18
  denumerable, 87
  empty, 16

Set (cont.)
  enumerable, 87
  finite, 16, 87
  infinite, 87
  of algebraic systems, directed, 98
    elementarily directed, 154
  of axioms for a class of systems, 157
  of conjunctive terms of a formula, 38
  of disjunctive terms of a formula, 38
  of formulas, compatible, 132
    consistent, 132
    incompatible, 132
  of formulas, inconsistent, 132
    locally satisfiable, 115
    satisfiable, 115
  of hypotheses, 53
  of natural numbers, 65
  of sentences, complete, 137
  recursive, 269
  recursively enumerable, 269
    m-universal, 275
  transitive, 84
Set-theoretic paradox, 9
Signature, of a class, 96
  of a class of algebraic systems, 157
Similarity, 76
Skolemization, of a signature, 166
  of a signature, complete, 167
  of an algebraic system, 166
  of an algebraic system, complete, 167
Subformula, 22, 104, 200
Subset, 15
Substitution, 32
Substitution theorem, 33
Subsystem, 98
  elementary, 153
  proper, 98
Subtree, 201
Subword, 17
Sum of a set, 85
Supersystem, 98
Symbol, 15
  auxiliary, 22
  logical, 22
  of a variable, 102
Syntax of a calculus, 44

Tautology, 119
Term, closed, 103
  of a sequence, 17
  recursive, 256
Theorem, of a calculus, 19
  of PC, 27
  on a graph, 265
  on the existence of a model, 133
  on the functional completeness of PC, 47
  on the omission of types, 173

Theory, 157, 165
  A_0, 283
    ∀-axiomatizable, 165
    √-axiomatizable, 165
    ∃-axiomatizable, 165
  axiomatizable, 287
  categorical, 188
  of an algebraic system, 149
  universally axiomatizable, 165
  with elimination of quantifiers, 166
Transfinite induction principle, 74
Tree, 27
Tree form proof in CP^{Σ}, 119
  in PC, 28
Triple, 18, 66
Truth function, 45
Truth value of a formula of PC, 45
Turing machine, 244
Turing's thesis, 246
Turnstile, 22
Type of a well-ordered set, 85
  of collection, 181

Ultrafilter, 81
Union of abstract words, 17
  of algebraic systems, 99
  of a set, 85
  of sets, 19, 20
Unit system, 162
Universal quantifier, 105
Upper bound, 70

Value, of a function, 69
  of a mapping, 18, 69
  of a term, 103
Variable, 102
  for formulas, 25, 118
  propositional, 22
Variety, 162

Well ordered set, 75
Word, 16, 65
  abstract, 16
  concrete, 16
  in an alphabet, 16

Yield sign, 22

Zermelo-Fraenkel axiom system, 92
  Σ-formula, 251
  Σ-term, 251
  ∀-formula, 159
  ∀∃-formula, 159
  ∃-formula, 159